

MODELLBASIERTE ENTSCHEIDUNGS-UNTERSTÜTZUNG FÜR VERTRAULICHKEIT UND DATENSCHUTZ IN GESCHÄFTSPROZESSEN
Sascha Alpers
KIT Scientific Publishing

Sascha Alpers

Modellbasierte Entscheidungsunterstützung für Vertraulichkeit und Datenschutz in Geschäftsprozessen

Modellbasierte Entscheidungsunterstützung für Vertraulichkeit und Datenschutz in Geschäftsprozessen

von

Sascha Alpers



Dissertation, Karlsruher Institut für Technologie
KIT-Fakultät für Wirtschaftswissenschaften

Tag der mündlichen Prüfung: 25. April 2019
Erster Gutachter: Prof. Dr. Andreas Oberweis
Zweite Gutachterin: Prof. Dr. Melanie Volkamer

Impressum



Karlsruher Institut für Technologie (KIT)
KIT Scientific Publishing
Straße am Forum 2
D-76131 Karlsruhe

KIT Scientific Publishing is a registered trademark
of Karlsruhe Institute of Technology.
Reprint using the book cover is not allowed.

www.ksp.kit.edu

Print on Demand 2019 – Gedruckt auf FSC-zertifiziertem Papier

ISBN 978-3-7315-0933-2
DOI 10.5445/KSP/1000094545

Modellbasierte Entscheidungs-unterstützung für Vertraulichkeit und Datenschutz in Geschäftsprozessen

zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften
(Dr.-Ing.)

von der KIT-Fakultät für Wirtschaftswissenschaften
des Karlsruher Instituts für Technologie (KIT)

genehmigte

DISSERTATION

von

Diplom-Informationswirt Sascha Alpers

Tag der mündlichen Prüfung: 25. April 2019
Erster Gutachter: Prof. Dr. Andreas Oberweis
Zweite Gutachterin: Prof. Dr. Melanie Volkamer

Vorwort

Diese Arbeit entstand während meiner Zeit als wissenschaftlicher Mitarbeiter im Forschungsbereich Software Engineering bzw. später zusätzlich als Leiter des Living Lab Software Innovations am FZI Forschungszentrum Informatik.

Mein Dank gilt ganz besonders meinem Doktorvater Herrn Prof. Dr. Andreas Oberweis für die engagierte Betreuung meiner Arbeit, die weiterführenden Anmerkungen und die konstruktiven Diskussionen. Von ihm habe ich gelernt, dass die Anfertigung der Arbeit (kurzfristig) nicht immer Spaß macht, aber (langfristig) zu Freude führt. Seine Art, mich zu betreuen, und sein Glaube an die Ideen der Arbeit waren eine starke Motivation für mich.

Ich bedanke mich ebenfalls bei Frau Prof. Dr. Melanie Volkamer für die Erstellung des Zweitgutachtens. Danken möchte ich auch Herrn Prof. Dr. Ralf Reussner (KIT-Fakultät für Informatik) für seine Mitwirkung an der Prüfung und Herrn Prof. Dr. Maxim Ulrich für die Übernahme des Prüfungsvorsitzes.

Herrn Prof. em. Dr. Dr. h. c. Wolffried Stucky danke ich für die Teilnahme an meinem Vortrag im Graduiertenkolloquium des KIT-Instituts AIFB und die zusätzlichen Anregungen, die aus seinen Fragen für die letzte Phase der Erstellung dieser Arbeit folgten.

Mein Dank gilt auch meinen Kolleginnen und Kollegen am FZI Forschungszentrum Informatik und in der Forschungsgruppe Betriebliche Informationssysteme am KIT-Institut AIFB für die gute Zusammenarbeit, die gemeinsamen Veröffentlichungen und die kollegialen Diskussionen. Meine (ehemaligen) Schreibtischnachbarinnen Esmahan Eryilmaz und Ainara Miller-Askar sowie die (ehemaligen) Kollegen Dr. Stefan Hellfeld, Prof. Dr. Thomas Schuster, Dr. David Karlin, Christoph Becker, Alexander Goranov, Oliver Denninger, Jörg Henss, Roman Pilipchuk, Maria Pieper und Jan Wiesenberger möchte ich an dieser Stelle hervorheben. Ich bedanke mich auch bei allen studentischen Hilfskräften und Abschlussarbeitern, die an einigen Aufgaben

von Forschungsprojekten mitgearbeitet und mir dadurch etwas Freiraum verschafft haben.

Ich bedanke mich weiter bei denen, die diese Arbeit Korrektur gelesen und mir dadurch geholfen haben, die sprachliche Verständlichkeit zu erhöhen.

Meinem Freundeskreis danke ich für das An-mich-Denken – auch wenn ich bedingt durch diese Arbeit einige Freizeitaktivitäten verpassen musste.

Die größte Unterstützung auf dem langen Weg zu dem Promotionsziel habe ich durch meine Familie erfahren. Auch ihr Glaube an meine Person hat mich weitergetragen. Herzlichen Dank für alle Unterstützung.

Ein Ziel ist erreicht. Aber auch von meinem Doktorvater Herrn Oberweis habe ich zugesprochen bekommen: „Das Schönste kommt noch“. Daran glaube ich gerne und ich freue mich auf dieses Geschenk.

Karlsruhe, im April 2019 Sascha Alpers

Kurzfassung

Organisationen müssen bzw. wollen Datenschutz und Vertraulichkeit als spezielle Anforderungen der IKT-Sicherheit gewährleisten. Es ist sinnvoll, Datenschutz und Vertraulichkeit nicht nur rein technisch zu betrachten, sondern diese bereits frühzeitig beim Entwurf von Geschäftsprozessen zu berücksichtigen, weil Informationen in Unternehmen typischerweise während der Ausführung von Geschäftsprozessen erhoben und verarbeitet werden.

Um Prozessmodellierer und -verantwortliche dabei zu unterstützen, wurden als graphisches Darstellungsmittel Informationsvertraulichkeits- und Datenschutz-Netze entwickelt. Diese erweiterten Petri-Netze ermöglichen es, Vertraulichkeit und Aspekte des Datenschutzes innerhalb von Geschäftsprozessmodellen systematisch zu betrachten. Dazu wird die Geschäftsprozesssicht insbesondere mit der Organisationsstruktursicht und der Datenstruktursicht zu einer integrierten Modellsicht verknüpft. Vertraulichkeit wird im Zusammenhang mit den an der Geschäftsprozessausführung beteiligten Ressourcen (Organisationsstruktur) und den zur Ausführung benötigten Daten (Datenstruktur) in Informationsvertraulichkeits- und Datenschutz-Netzen entweder klassen- oder rollenbasiert betrachtet. Zweckbindung und Datenminimierung als spezielle Aspekte des Datenschutzes können mittels der Informationsvertraulichkeits- und Datenschutz-Netze ebenfalls beschrieben werden. Informationsvertraulichkeits- und Datenschutz-Netze wurden so definiert, dass Simulations- und Analysemethoden von traditionellen Petri-Netzen angewandt beziehungsweise übertragen werden können. So können Aussagen getroffen werden, wie sich bestimmte Anforderungen der Vertraulichkeit beziehungsweise des Datenschutzes auf Geschäftsprozesse und ihre Ausführung auswirken.

Um die Anwendung zu unterstützen, wird die neue PriCon4BPM-Methode (Privacy & Confidentiality for Business Process Management) vorgeschlagen. Dabei werden die Schritte zur Erstellung der Informationsvertraulichkeits- und Datenschutz-Netze de-

tailliert beschrieben. Zusätzlich wird eine durchgängige Vorgehensweise von der Modellierung bis zur Entscheidung (beispielsweise bezüglich Prozessalternativen) vorgestellt.

Inhaltsverzeichnis

Vorwort i

Kurzfassung iii

Abbildungsverzeichnis vii

Tabellenverzeichnis ix

Verzeichnis der Definitionen xi

1 Einleitung 1
1.1 Ausgangssituation 1
1.2 Zielsetzung der Arbeit 4
1.3 Aufbau der Arbeit 6

2 Grundlagen: Sicherheit 11
2.1 Schutzziele der Informationssicherheit 13
2.2 Vertraulichkeit 23
2.3 Sicherheitsökonomie und Risikomanagement 25

3 Grundlagen: Datenschutz 31
3.1 Geschichte des Datenschutzrechtes 32
3.2 Bedeutung des Datenschutzes 40
3.3 Anwendungsbereich EU-DS-GVO 45
3.3.1 Sachlicher Anwendungsbereich 45
3.3.2 Räumlicher Anwendungsbereich 50
3.4 Grundsätze des Datenschutzes der EU-DS-GVO 51
3.4.1 Rechtmäßigkeit 51
3.4.2 Verarbeitung nach Treu und Glauben 60
3.4.3 Transparenz 60
3.4.4 Zweckbindung 61
3.4.5 Datenminimierung 63
3.4.6 Richtigkeit 64
3.4.7 Speicherbegrenzung 64
3.4.8 Vertraulichkeit und Integrität 64
3.4.9 Rechenschaftspflicht 65

4 Grundlagen: Unternehmensmodellierung ... 67
4.1 Modellierung ... 67
4.2 Sichten auf ein Unternehmen ... 73
4.3 Die Geschäftsprozesssicht ... 74
4.3.1 Petri-Netze ... 78
4.3.2 Workflow-Netze ... 84
4.3.3 Analysemethoden für Petri-Netze ... 85
5 Informationsvertraulichkeits- und Datenschutz-Netze ... 87
5.1 Informationsvertraulichkeit ... 88
5.1.1 Klassenbasierte Informationsvertraulichkeit ... 90
5.1.2 Rollenbasierte Informationsvertraulichkeit ... 103
5.2 Datenschutz ... 109
5.2.1 Zweckbindung ... 111
5.2.2 Datenminimierung ... 116
5.3 Informationsvertraulichkeits- und Datenschutz-Netz ... 118
6 Simulations- und Analyseverfahren für Informationsvertraulichkeits- und Datenschutz Netze ... 125
6.1 Fragestellungen ... 126
6.2 Simulation ... 126
6.3 ICPN-Sim ... 136
6.4 Simulationsprotokoll ICPN-Trace ... 138
6.5 Auswertung der Simulation ... 144
7 Die PriCon4BPM-Methode ... 147
7.1 BPM-LifeCycle-Management ... 147
7.2 Eigene Methode ... 150
7.3 Anwendungsbeispiel ... 158
8 Einordnung der PriCon4BPM-Methode ... 179
8.1 Anforderungen ... 179
8.2 Eigene und verwandte Arbeiten ... 182
8.3 Anwendbarkeit ... 184
9 Fazit und Ausblick ... 187
9.1 Fazit ... 187
9.2 Ausblick ... 192
10 Literaturverzeichnis ... 195

Abbildungsverzeichnis

Abbildung 1: Schutzziele der Informationssicherheit ... 17

Abbildung 2: Dateninteressent und dadurch in ihren Rechten bedrohte Datenquelle ... 46

Abbildung 3: Grundsätze zur Verarbeitung personenbezogener Daten nach Artikel 5 EU-DSG-VO ... 52

Abbildung 4: Zusammenhang Modelloriginal und Modell ... 71

Abbildung 5: Sichten der Unternehmensmodellierung ... 73

Abbildung 6: Symbole für Stelle, Transition und gerichtete Kante ... 78

Abbildung 7: Petri-Netz vor (links) und nach (rechts) Schalten der Transition ... 81

Abbildung 8: Sequenzielle, alternative und nebenläufige Ausführung in Petri-Netzen ... 83

Abbildung 9: Übersicht der verschiedenen Netze ... 87

Abbildung 10: beispielhafter Ausschnitt eines einfachen klassenbasierten Informationsvertraulichkeits-Netzes ... 94

Abbildung 11: Informationsvertraulichkeits-Netz zur Darstellung einer Bestellabwicklung ... 101

Abbildung 12: vereinfachte Darstellung ausgewählter Rahmenbedingungen an die Verarbeitung personenbezogener Daten ... 111

Abbildung 13: Beispiel für ein Zweckbindungs-Netz ... 116

Abbildung 14: Beispiel für eine deterministische Simulation ... 128

Abbildung 15: Beispiel einer stochastischen Simulation mit zwei möglichen Simulationsergebnissen ... 130

Abbildung 16: Markierungsgraph zum Petri-Netz aus Abbildung 15 mit Anfangsmarkierung m0 ... 131

Abbildung 17: Beispiel für ein Petri-Netz mit Anfangsmarkierung m0, endlichem Markierungsgraphen und unendlicher Menge an möglichen Simulationsergebnissen ... 133

Abbildung 18: Petri-Netz mit Anfangsmarkierung m0 mit resultierendem unendlichem Markierungsgraphen, ausschnittsweise dargestellt ... 135

Abbildung 19: Darstellung des Simulationsablaufes ... 138

Abbildung 20: Lebenszyklusphasen des Geschäftsprozessmanagements ... 148

Abbildung 21: Ziel und Bestandteile einer Methode 150
Abbildung 22: Ausschnitt aus dem Vorgehensmodell der PriCon4BPM-Methode . 154
Abbildung 23: Verfeinerung der Aktivität „Aktivität beschreiben“ 155
Abbildung 24: angepasster Lebenszyklus des Geschäftsprozessmanagements 157
Abbildung 25: Informationsobjekttypmodell zum Anwendungsbeispiel; modelliert mittels Horus 175
Abbildung 26: Bestellprozess als Informations- und Vertraulichkeits-Netz 176

Tabellenverzeichnis

Tabelle 1: Zuordnung von Bedrohungen zu typischen Ursachen und typischen / primär bedrohten Schutzzielen 19
Tabelle 2: Ordinalskala für die Informationsvertraulichkeitsklassifikation 91
Tabelle 3: Ordinalskala für die Vertrauenswürdigkeitsklassifikation von Ressourcen 92
Tabelle 4: Beispielschaltfolge 1 102
Tabelle 5: Beispielschaltfolge 2 102
Tabelle 6: Vergleich verschiedener Ansätze hinsichtlich der Anforderungen 183

Verzeichnis der Definitionen

Definition 2.1: Informationsvertraulichkeit ... 25
Definition 3.1: personenbezogene Daten ... 48
Definition 3.2: Einwilligung ... 53
Definition 3.3: besondere Kategorien personenbezogener Daten ... 56
Definition 4.1: Modell, Modelloriginal, Sicht und Modellierung ... 68
Definition 4.2: Modell-Suite ... 72
Definition 4.3: Geschäftsprozess ... 76
Definition 4.4: Geschäftsprozessmodell ... 77
Definition 4.5: Geschäftsprozessinstanz ... 77
Definition 4.6: Petri-Netz ... 79
Definition 4.7: Markierung eines Petri-Netzes ... 80
Definition 4.8: Vor- und Nachbereich einer Transition in einem Petri-Netz ... 80
Definition 4.9: Vor- und Nachbereich einer Stelle in einem Petri-Netz ... 80
Definition 4.10: Schaltregel ... 81
Definition 4.11: Pfad ... 83
Definition 4.12: streng zusammenhängend ... 84
Definition 4.13: Workflow-Netz ... 85
Definition 4.14: Erreichbarkeit ... 85
Definition 4.15: Erreichbarkeitsmenge ... 86
Definition 5.1: klassenbasiertes Informationsvertraulichkeits-Netz ... 93
Definition 5.2: Markierung eines klassenbasierten Informationsvertraulichkeits-Netzes ... 95
Definition 5.3: Informationsvertraulichkeit einer Stelle ... 95
Definition 5.4: Vertrauenswürdigkeit einer Transition ... 96
Definition 5.5: klassenbasierte Ablauf-Informationsvertraulichkeit ... 99
Definition 5.6: Informationsvertraulichkeits-Netz ... 104
Definition 5.7: Verknüpfung von Mengensystemen ... 106
Definition 5.8: Rollenmengensystem mit Zugriff auf eine Stelle ... 107

Definition 5.9: Ablauf-Informationsvertraulichkeit 108
Definition 5.10: Zweckbindungs-Netz 112
Definition 5.11: Markierung eines Zweckbindungs-Netzes 113
Definition 5.12: Schaltregel mit Berücksichtigung der Zweckbindung im Ablauf .. 115
Definition 5.13: Petri-Netz mit Annotationen zur Analyse der Datenminimierung 117
Definition 5.14: Informationsvertraulichkeits- und Datenschutz-Netz 119
Definition 5.15: Markierung eines Informationsvertraulichkeits- und Datenschutz-Netzes 120
Definition 5.16: Schaltregel mit Berücksichtigung der Zweckbindung und Informationsvertraulichkeit im Ablauf 122
Definition 6.1: Simulation 127

1 Einleitung

In diesem Kapitel werden zunächst die Ausgangssituation und die Motivation für die vorliegende Arbeit erläutert. Es folgt eine Beschreibung der Zielsetzung und des Aufbaus der Arbeit.

1.1 Ausgangssituation

Effektive und effiziente Geschäftsprozesse sind ein wesentlicher Erfolgsfaktor für die Wertschöpfung in Unternehmen. Dabei wird eine besonders hohe Effektivität, also eine hohe Quote der Erreichung des tatsächlichen Zieles, in der Regel vorausgesetzt. Prozessverantwortliche und -designer müssen beispielsweise aufgrund des zunehmenden Wettbewerbsdrucks oder aufgrund steigender Renditeerwartungen zusätzlich aber immer weitere Effizienzsteigerungen erreichen. Das heißt, der Aufwand, der zur Zielerreichung erbracht wird, muss in der Regel ohne Beeinträchtigung der Effektivität reduziert werden. Effizienzsteigerungen werden durch die Gestaltung vollständig neuer Prozesse und die kontinuierliche Verbesserung vorhandener Prozesse erreicht.

Gleichzeitig nimmt die Bedeutung von Sicherheit für Unternehmen weiter zu (Bundesdruckerei & Kantar Emnid, 2017). Sicherheit umfasst im Kontext von Prozessen zunehmend mehr Aspekte. Typische Beispiele sind die Einhaltung der Vorschriften des Arbeits- und Umweltschutzes sowie vorhandener Prozessregeln (zum Beispiel Vieraugenprinzip). Eine weitere wichtige Anforderung ist, dass Unternehmensgeheimnisse sowie Kunden- und Mitarbeiterdaten geschützt werden und deren Integrität sichergestellt wird. Mittlerweile muss nicht nur von einer theoretischen Gefährdung ausgegangen werden. Das Interesse von Dritten an diesen Informationen ist real, und ihre technischen Möglichkeiten sind enorm. Dabei werden Unternehmen nicht nur mit kriminellen Einzelabsichten (zum Beispiel Identitätsdiebstahl, Berei-

cherung mittels Kreditkartendaten), sondern auch zur Erreichung von Wettbewerbsvorteilen und zur Stärkung von Verhandlungspositionen (Industriespionage) angegriffen. Hinsichtlich der Globalisierung von Informationen können Unternehmen nicht mehr davon ausgehen, dass ein einzelner Rechtsstaat ihre Informationen ausreichend durch Gesetze und Strafverfolgung schützen kann. Die Verantwortung liegt folglich im Unternehmen selbst. Auch die Zuverlässigkeit der Prozesse, beispielsweise die zeitgerechte Bereitstellung von Ergebnissen, ist von großer Bedeutung. Aufgrund der zunehmenden Verbreitung von Lean-Methoden und speziell des Just-in-time-Prinzips werden Puffer abgebaut und die Auswirkungen von möglichen Prozessstörungen in vielen Fällen vergrößert (vgl. Tortorella, Miorando & Marodin, 2017). Es wird also erwartet, dass effektive und effiziente Prozesse zusätzlich auch sicher sind, damit die Zukunftsfähigkeit des Unternehmens und seiner Wertschöpfung nicht unbeabsichtigt Gefahren ausgesetzt ist.

Ein potenzielles Angriffsziel ist die im Rahmen der Prozessausführung verwendete Informations- und Kommunikationstechnologie (IKT) – unabhängig davon, ob sie vom Unternehmen selbst betrieben oder von Dienstleistern bereitgestellt wird. Oft wird daher gefordert, die IKT solle maximal beziehungsweise best möglich sicher sein (Weppler, 2016). Dadurch wird die Verantwortung an die Unternehmens-IT delegiert, die diese Aufgabe zumeist losgelöst von den eigentlichen Wertschöpfungsprozessen erfüllt. Zum Nachweis der Sicherheit beziehungsweise der Bemühungen darum erwerben Unternehmen in der Regel verschiedene Zertifikate (zum Beispiel nach ISO 27001). Das Paradigma, die Sicherheit der eingesetzten IT isoliert von den Prozessen zu betrachten und ein möglichst hohes Schutzniveau zu fordern, ist gegenwärtig ein gängiger Ansatz, um die beschriebenen Forderungen umzusetzen beziehungsweise den erwähnten Gefahren zu begegnen (vgl. Sowa, 2017). Durch unternehmensübergreifende Leistungserbringung und die zunehmende Integration von mobilen Endgeräten wird dies jedoch zu einer immer komplexeren Aufgabe und einem wachsenden Kostenfaktor für die Unternehmen. Die Kosten, die im Rahmen der Absicherung der Geschäftsprozesse anfallen, beeinflussen auch die Kosten der

Wertschöpfungsprozesse und müssen auf diese umgelegt werden. Somit wird auch die Effizienz der Prozesse davon beeinflusst.

Auch die Auswirkungen des Datenschutzes auf Geschäftsprozesse haben zugenommen. Unternehmen sind durch die Europäische Datenschutzgrundverordnung (EU-DSGVO) und insbesondere durch die darin festgelegten möglichen Sanktionen für Datenschutz aktuell besonders sensibel. Dabei stehen sie im Spannungsfeld zwischen der betroffenenfreundlichen, minimal notwendigen Datenverarbeitung (im Idealfall ausschließlich, soweit es notwendig ist, um Verträge mit dem Betroffenen zu erfüllen) und einem wirtschaftlichen Wert von möglichst vielen personenbezogenen Daten – wobei eine datenschutzkonforme Monetisierung für neue Marktteilnehmer eine Herausforderung darstellt (vgl. Leutheusser-Schnarrenberger, 2016). Da „Organisationen, die mit personenbezogenen Daten arbeiten, […] die ihnen anvertrauten Informationen häufig gern weitaus intensiver nutzen [würden], als sie es aus datenschutzrechtlichen Gründen dürfen […] erscheint Datenschutz […] auch aus wirtschaftlicher Sicht häufig als ‚Sand im Getriebe'" (<kes>, 2018 S. 49). Andererseits sind auch besonders datenschutzfreundliche Dienstleister für bestimmte Kunden (Privatpersonen und andere Unternehmen) attraktiv, sodass auch daraus ein Wettbewerbsvorteil entstehen kann. Hierzu muss jedoch künftig ein signifikanter Anteil der potenziellen Kunden für das Thema Datenschutz sensibilisiert sein (Appl u. a., 2017). In jedem Fall muss Datenschutz beim Entwurf von Geschäftsprozessen beachtet werden, wenn diese personenbezogene Daten verarbeiten.

Durch die isolierte Wahrnehmung der Aufgaben (Prozessverantwortung/-design und IKT-Sicherheit sowie Datenschutz) wird einerseits eine höhere Spezialisierung und damit eine hohe Effizienz der Teilaufgaben erreicht, andererseits verlieren die beteiligten Spezialisten das Bewusstsein für die Auswirkungen ihrer Entscheidungen auf die jeweils andere Aufgabe. B. Weßelmann und J. Wiele beschreiben die Situation in vielen Organisationen wie folgt: „Manchmal behindern sich die beiden Fachabteilungen [Datenschutz und Security] gegenseitig bei ihren Projekten, manchmal wird die

Blockade des einen sogar zum ‚Showstopper' für die Bemühungen des anderen" (<kes>, 2018, S. 48).

Wenn Fragestellungen der Sicherheit und im Speziellen der IKT-Sicherheit und Fragestellungen des Datenschutzes bereits bei der Gestaltung der Prozesse berücksichtigt werden, können Designalternativen auch hinsichtlich ihrer Sicherheitsrisiken beziehungsweise -kosten und der Datenschutzkonformität beziehungsweise -freundlichkeit bewertet werden. Zudem kann differenzierter betrachtet werden, welche Sicherheitsanforderungen beziehungsweise Datenschutzanforderungen für welche Prozessschritte und Objekte überhaupt relevant sind. Maßnahmen der IKT-Sicherheit und des Datenschutzes können somit gezielter erfolgen. Eine integrierte Betrachtung ist folglich wirtschaftlich sinnvoll, sofern Maßnahmen durch geeignete Verfahren und Werkzeuge unterstützt und daher ermöglicht werden.

1.2 Zielsetzung der Arbeit

Das Ziel der vorliegenden Arbeit ist es, eine modellbasierte Entscheidungsunterstützung zur Planung und Umsetzung von IKT-Sicherheit und Datenschutz in Geschäftsprozessen zu realisieren. Beide Bereiche zu betrachten liegt nahe, weil IKT-Sicherheit die Einhaltung des Datenschutzes fördert (vgl. Zeuner, 2016).

Da dies beides weitere Themenfelder sind, soll die vorliegende Arbeit auf den Aspekt Informationsvertraulichkeit der IKT-Sicherheit und auf die Grundsätze Zweckbindung und Datenminimierung des Datenschutzes fokussieren. Dabei soll nicht das Ziel maximaler Sicherheit im Blickpunkt stehen, sondern es soll ein wirtschaftlicher, d. h. angemessene Sicherheitsgrad erreicht werden. Bezüglich des Datenschutzes sollen Verantwortliche unterstützt werden, datenschutzfreundliche und datenschutzrechtskonforme Geschäftsprozesse zu entwerfen.

Teilziele sind eine formalisierte Modellierung der Informationsvertraulichkeits- sowie Zweckbindungsanforderungen und eine systematische, modellbasierte Betrachtung des Datenminimierungsprinzips.

Im Hinblick auf die Informationsvertraulichkeit bedeutet dies, dass es zunächst ermöglicht werden muss, Anforderungen der Informationsvertraulichkeit in die Prozessmodellierung zu integrieren, damit Prozessverantwortliche und -designer die Anforderungen dermaßen gestalten können, dass sie den Notwendigkeiten einzelner Prozesse und Prozessschritte entsprechen. Da Anforderungen bezüglich der Vertraulichkeit oft mit einzelnen Informationsobjekten zusammenhängen, muss auch eine Verknüpfung zwischen Anforderung und Informationsobjekt möglich sein. Durch die integrierte Modellierung sollen die Anforderungen für alle Beteiligten transparent werden. Somit wird der Austausch über diese Anforderungen ermöglicht und gefördert. Die Möglichkeit der informationsobjektzentrierten Modellierung der Sicherheitsanforderungen erleichtert den Beteiligten das Verständnis, weil es den aufgrund der bisherigen Umsetzungstechniken vorhandenen Denkmustern bezüglich Vertraulichkeit entspricht.

Hinsichtlich des Datenschutzes werden die Grundsätze Zweckbindung und Datenminimierung betrachtet. Dabei muss es Prozess- und Datenschutzverantwortlichen ermöglicht werden, die Auswirkungen des Geschäftsprozesses auf die Daten von natürlichen Personen zu betrachten. Hier kann es ein Ziel sein, einen möglichst datenschutzfreundlichen Geschäftsprozess zu schaffen, der beispielsweise durch besonders datensparsame Prozessschritte über regulatorische Vorgaben hinausgeht. Dazu muss aber mindestens ein datenschutzrechtlich konformer Geschäftsprozess erstellt werden.

Die formalisierte Modellierung der Anforderungen ist zudem eine notwendige Grundlage für eine weitere systematische Betrachtung. Dazu müssen Analyse- und Simulationsverfahren bereitgestellt werden, welche die Auswirkungen der Anforderungen auf den Prozess aufdecken und beschreiben. Dabei sind auch Wechselwirkungen zwischen verschiedenen, sich gegenseitig beeinflussenden Anforderungen zu berücksichtigen. Relevante Fragestellungen betreffen beispielsweise die Ausführbarkeit des Prozesses oder die Notwendigkeit der verwendeten Daten für einzelne Akteure beziehungsweise Aktionen.

Darüber hinaus benötigen Prozessverantwortliche und -modellierer methodische Unterstützung zur strukturierten Betrachtung von Informationsvertraulichkeit, Zweckbindung und Datenschutz im Rahmen des Geschäftsprozessdesigns. Dabei bilden, wie schon erörtert, die drei Anforderungsbereiche nur Teile der größeren Bereiche IKT-Sicherheit und Datenschutz ab. Sprache und Methode sollten später also hinsichtlich weiterer Bereiche erweitert werden können.

Über die Beschränkung dieser Arbeit auf die drei Anforderungsbereiche hinaus müssen weitere Einschränkungen vorgenommen werden. Beispielsweise werden physische Gefahren, wie ein möglicher Diebstahl von Datenträgern nach Einbruch in ein Rechenzentrum, nicht betrachtet. Genauso wenig wird die technische Umsetzung der Geschäftsprozesse, das heißt ihre Implementierung, untersucht. Der Ansatz bleibt auf der Ebene des Geschäftsprozessentwurfs und ist an Prozessverantwortliche und -modellierer gerichtet, welche Informationsvertraulichkeit und Datenschutz umsetzen möchten.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit ist wie folgt strukturiert:

Das nachfolgende zweite Kapitel befasst sich mit Sicherheitsanforderungen in Organisationen. Hierzu wird zunächst der Begriff „Sicherheit" näher untersucht. Es werden sogenannte Schutzziele aus der Literatur beschrieben und kategorisiert. Darauf aufbauend werden 47 elementare Bedrohungen den fünf Hauptschutzzielen Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Rechtsverbindlichkeit zugeordnet. Anschließend wird das Schutzziel der Vertraulichkeit näher betrachtet und das Teilziel der Informationsvertraulichkeit, also des Schutzes der Informationsinhalte, herausgearbeitet. Im weiteren Verlauf der vorliegenden Arbeit wird dann bezüglich der Schutzziele der Informationssicherheit auf das Schutzziel Informationsvertraulichkeit fokussiert. Das Kapitel schließt mit Grundlagen zur Sicherheitsökonomie.

Das dritte Kapitel widmet sich den Grundlagen des Datenschutzes. Weil die aktuelle Rechtsgrundlage relativ neu und somit ihre Auslegung noch nicht in allen Bereichen klar ist, wird zunächst die Geschichte des Datenschutzrechtes betrachtet, bevor dann die Bedeutung des Datenschutzes für die Gesellschaft herausgearbeitet wird. Im Anschluss werden der Anwendungsbereich und die neun Grundsätze der Europäischen Datenschutz-Grundverordnung erläutert. Dabei wird im Abschnitt Rechtmäßigkeit auch definiert, was personenbezogene Daten sind, bevor mit Zweckbindung und Datenminimierung auch die für die vorliegende Arbeit besonders wichtigen Grundsätze erörtert werden.

Nachdem in den beiden vorangehenden Kapiteln die fachlichen Grundlagen für die Erweiterung einer Modellierungssprache gelegt wurden, werden im vierten Kapitel die methodischen und sprachlichen Grundlagen der Unternehmensmodellierung charakterisiert. Hierzu werden die Begriffe „Modell“ und „Modellierung“ definiert, und es wird ausgeführt, welche verschiedenen Sichten es auf ein Unternehmen geben kann. Im Anschluss wird die Geschäftsprozesssicht als eine verhaltensbezogene Sicht auf ein Unternehmen dargestellt, bevor die Modellierungssprache Petri-Netze vorgestellt wird. Darauf aufbauend werden Workflow-Netze (eine Teilmenge von Petri-Netzen) sowie Analysemethoden für Petri-Netze vorgestellt.

Im fünften Kapitel werden Informationsvertraulichkeits- und Datenschutz-Netze dargestellt. Das Kapitel ist in drei Unterkapitel aufgeteilt. Im ersten Unterkapitel wird die Informationsvertraulichkeit betrachtet. Zunächst wird eine Erweiterung von höheren Petri-Netzen zur Modellierung von klassenbasierter Informationsvertraulichkeit beschrieben. Hierzu wird zunächst das klassenbasierte Informationsvertraulichkeits-Netz definiert, bevor anschließend Markierung, Vertrauenswürdigkeit einer Transition und Vertraulichkeit einer Stelle erläutert werden. Darauf aufbauend wird dann die Schaltregel erörtert. Für die rollenbasierte Informationsvertraulichkeit wird eine entsprechende Erweiterung beschrieben. Im zweiten Unterkapitel wird für den Datenschutzgrundsatz Zweckbindung eine Erweiterung veranschaulicht. Der Ansatz ermöglicht es, mit speziellen Transitionen erlaubte Verarbeitungszwecke mit

Informationsobjekten zu verknüpfen. Anschließend werden zusätzliche Bedingungen für das Schalten von Transitionen eingeführt, welche zur Laufzeit die Zweckbindung überwachen. Für den Grundsatz der Datenminimierung wird eine Möglichkeit vorgestellt, Transitionen so zu annotieren, dass später untersucht werden kann, welche Daten minimal benötigt werden. Im dritten Unterkapitel werden die verschiedenen Spracherweiterungen zu Informationsvertraulichkeits- und Datenschutz-Netzen zusammengeführt.

Das sechste Kapitel beschreibt, wie mittels der vorgestellten Spracherweiterung modellierte Prozesse analysiert beziehungsweise simuliert werden können. Hierzu werden zunächst die Fragestellungen aufgelistet, welche mithilfe einer systematischen Analyse der Modelle beantwortet werden sollen. Im Anschluss daran werden die Simulationsstrategie für Informationsvertraulichkeits- und Datenschutz-Netze festgelegt und das Simulationsverfahren schrittweise erläutert. Damit sowohl die Simulationsparameter als auch die Simulationsergebnisse strukturiert und auswertbar festgehalten werden können, wird ein XML-Dialekt als Sprache für das Simulationsprotokoll artikuliert. Das Kapitel schließt mit einer Beschreibung, wie die zu Beginn des Kapitels aufgelisteten Fragen mithilfe der Simulation beantwortet werden können.

Im siebten Kapitel wird die PriCon4BPM-Methode erklärt. Dazu wird zunächst der BPM-LifeCycle erörtert, um anschließend die neue Methode einordnen zu können. Diese wird dann im zweiten Unterkapitel vorgestellt. Hierzu werden zunächst die Aktivitäten der Methode definiert, und für einige Aktivitäten werden Techniken bereitgestellt. Die Aktivitäten werden hierauf in ein Vorgehensmodell eingeordnet. Schließlich werden die Ergebnisartefakte beschrieben. In der vorliegenden Arbeit wurden dafür teils eigene Sprachen entwickelt. Ein Anwendungsbeispiel beschließt das Kapitel und hilft beim weiteren Verständnis der Methode.

Im achten Kapitel wird die PriCon4BPM-Methode in die Literatur eingeordnet. Zu diesem Zweck werden zunächst die Anforderungen aus der Einleitung präzisiert und dann die Erfüllung der Anforderungen von PriCon4BPM mit anderen Ansätzen aus

der Literatur verglichen. Hierzu wird auf eine bereits publizierte Literaturrecherche zurückgegriffen. Letztlich wird die Anwendbarkeit der Methode anhand verschiedener Beispiele aufgezeigt.

Das neunte Kapitel enthält eine Zusammenfassung der Ergebnisse der vorigen Kapitel. Die Ergebnisse werden kritisch bewertet und mögliche zukünftige Forschungsfragen werden erörtert.

2 Grundlagen: Sicherheit

Zunächst muss bestimmt werden, was in dieser Arbeit unter dem Begriff „Sicherheit“ verstanden wird, weil der Begriff verschiedene Bedeutungen hat. So wird im deutschen Sprachgebrauch Sicherheit sowohl für den Begriff „safety“ als auch für den Begriff „security“ aus der internationalen Literatur verwendet. Die Begriffe können wie folgt inhaltlich unterschieden werden:

- Safety bezeichnet nach Pohl (H. Pohl, 2004) den „Zustand eines Systems, in dem Maßnahmen zum Schutz (zur Vermeidung von Schäden) wirksam sind. In diesem Zustand ist das System frei von [...] Gefahren, die dem System oder (außerhalb:) der Umwelt drohen – gekennzeichnet durch Begriffe wie Betriebssicherheit und Arbeitssicherheit“. Der Begriff System meint in der Veröffentlichung von Pohl (H. Pohl, 2004) ein IT-System.
- Security bezeichnet einen Zustand eines Systems, in dem das System durch Maßnahmen vor „unerwünschtem Verhalten“ der Umgebung geschützt ist (H. Pohl, 2004). Dabei spielt es zunächst keine Rolle, ob ein Angreifer absichtlich dieses unerwünschte Verhalten ausführt oder jemand unabsichtlich das falsche Verhalten ausführt.

So gehört der Anschnallgurt im Flugzeug zum Bereich der Safety, die Passagier- und Gepäckkontrollen am Flughafen zu Security. Das Beispiel vom Flughafen beziehungsweise Flugzeug zeigt auch den Aspekt des Angreifers im Falle von Security. Die Kontrollen wurden eingeführt, nachdem es in den 1970er-Jahren mehrere Flugzeugentführungen gab, es wurde also auf konkrete Gefahren durch vergangene Angreifer reagiert (Harms, 2011). Im Falle von Safety spielen Angriffe dagegen i. d. R. keine Rolle, vielmehr wurde die Gurtpflicht aufgrund von Unfällen eingeführt (Bergmann, 2009).

Nach Dierstein (Dierstein, 2004) sind die englischen Begriffe in der Diskussion um den Sicherheitsbegriff „zwar anwendbar, aber wenig geeignet". Der wesentliche Unterschied zwischen beiden Begriffen wäre durch die intentionalen Beeinträchtigungen (Security) und nichtintentionalen Beeinträchtigungen (Safety) gegeben. Da es bei der Beurteilung des Schadens nicht auf vorhandene beziehungsweise nicht vorhandene Absicht ankommt, sei die Unterscheidung mit dieser Bedeutung nicht zielführend.

Eckert (Eckert, 2018) unterscheidet im Zusammenhang mit der Sicherheit von IT-Systemen jedoch ebenfalls diese Begriffe – allerdings mit anderem Schwerpunkt. So wird Safety als Funktionssicherheit von Security als Informationssicherheit abgegrenzt.

- Die Funktionssicherheit (Safety) ist die Eigenschaft eines Systems, „dass die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt. Ein funktionssicheres System nimmt keine funktional unzulässigen Zustände an" (Eckert, 2018, S. 6). Auch wenn der Schwerpunkt in dieser Definition im Gegensatz zu Pohl (H. Pohl, 2004) nicht auf dem Schutz des Systems liegt, wird doch deutlich, dass das System spezifikationsgemäß funktionieren soll und damit weder Umwelt noch das System selbst gefährdet sein sollen.
- Nach Eckert (Eckert, 2018, S. 6) bezeichnet Informationssicherheit (Security) „die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen".

Wenn man die Definitionen zusammennimmt, wird Security als Sicherheit gegenüber absichtlichen Angriffen (Dierstein, 2004) der Umgebung (H. Pohl, 2004) verstanden, die dazu führt, dass ein System keine unautorisierte Informationsveränderung beziehungsweise Informationsgewinnung zulässt (Eckert, 2018). Dementsprechend kann Safety als Sicherheit vor nicht absichtlichen Aktionen (Dierstein, 2004) des Systems mit Schäden für die Umgebung oder das System selbst (H. Pohl, 2004) bezeichnet

werden. Es wird also garantiert, dass die „Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt“ (Eckert, 2018, S. 6).

In dieser Arbeit wird Vertraulichkeit als ein Schutzziel betrachtet. Dabei ist es – analog zu Dierstein (Dierstein, 2004) – nicht relevant, ob es dem Begriff Security und/oder dem Begriff Safety zuzuordnen ist. In jedem Fall ist das Schutzziel der Vertraulichkeit aber in weitere Schutzziele, insbesondere dem der Informationssicherheit, eingebettet. Daher werden zur Abgrenzung im ersten Unterkapitel die Schutzziele der Informationssicherheit insgesamt dargestellt, bevor im zweiten Unterkapitel das Schutzziel der Vertraulichkeit genauer betrachtet wird.

2.1 Schutzziele der Informationssicherheit

Pohl (H. Pohl, 2004) nimmt eine Taxonomie für den Begriff Informationssicherheit vor. Dort werden vier unabhängige, orthogonale Schutzziele mit insgesamt bis zu zwölf Unterschutzzielen zur Definition der Zielsetzung von Informationssicherheit im engeren Sinne (das heißt von „IT-Sicherheit“) herangezogen. Diese sind:

1. Vertraulichkeit
2. Integrität
    a. Konsistenz
    b. Genauigkeit
    c. Korrektheit
    d. Vollständigkeit
    e. (Plausibilität)[1]
3. Verfügbarkeit
    a. Zuverlässigkeit

[1] Dieses Schutzziel ist in der grafischen Abbildung der Schutzziele (H. Pohl, 2004, Abbildung 4) nicht enthalten, wird im Text der Veröffentlichung aber als Unterpunkt von Integrität genannt.

   b. Fehlertoleranz
   c. Robustheit
   d. Wiederherstellbarkeit
   e. (Flexibilität)[2]
4. Verbindlichkeit
   a. Authentizität
   b. Beherrschbarkeit

Pohl (H. Pohl, 2004) beschreibt auch das (Teil-)Schutzziel der „Revisionsfähigkeit“, ordnet es aber keinem der vier genannten Hauptziele zu. Die Zuordnung ist auch nicht eindeutig, weil Revisionsfähigkeit beispielsweise Integrität (unveränderte Daten) und Verbindlichkeit (hier als Möglichkeit, Handlungen auf einen Akteur zurückzuverfolgen) voraussetzt.

Einige Schutzziele, wie Integrität, können nur ganz oder gar nicht erreicht werden (binäre Ziele); bei anderen Schutzzielen, wie Verfügbarkeit, können unterschiedliche Niveaus erreicht beziehungsweise unterschieden werden (H. Pohl, 2004).

Das Bundesamt für Sicherheit in der Informationstechnik gab 2018 erstmals das IT-Grundschutz-Kompendium als Nachfolger der IT-Grundschutz-Kataloge heraus. Darin werden drei Hauptziele genannt: Vertraulichkeit, Integrität und Verfügbarkeit (BSI, 2018, S. 1). Verbindlichkeit wird darin nicht explizit erwähnt. Vollständig sind weder die vier noch die drei Schutzziele. Die Aufzählung gibt trotz des Fehlens weiterer, je nach Szenario relevanter, Schutzziele, wie Anonymität, Pseudonymität, Unbeobachtbarkeit, Nicht-Vermehrbarkeit (H. Pohl, 2004, Abbildung 5) und Wartbarkeit (Dierstein, 2004), mit ihren drei (nach BSI, 2018) beziehungsweise vier (nach H. Pohl, 2004) Schutzzielen bereits ein häufiges Verständnis der Ziele von Informationssicherheit wieder.

[2] Pohl (H. Pohl, 2004) beschreibt dies als nicht notwendige, aber unterstützende Eigenschaft. Im Ansatz von Bedner & Ackermann (Bedner & Ackermann, 2010) müsste das Ziel dem dort vorhandenen Hauptziel der Kontingenz zugeordnet werden.

Die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit finden sich auch bei Bedner & Ackermann (Bedner & Ackermann, 2010) und werden dort um die zwei weiteren Schutzziele Kontingenz und Transparenz ergänzt. Kontingenz soll als „ein Schutzziel gegen Einengung durch Technik“ wirken und verhindern, durch „Technikeinsatz ohne Interventionsmöglichkeit eingeengt zu werden“ (Bedner & Ackermann, 2010). Dazu gehört das Unterziel der glaubhaften Abstreitbarkeit. Transparenz ist mit dem Schutzziel „Verbindlichkeit“ nach Pohl (H. Pohl, 2004) vergleichbar, zumal Bedner & Ackermann (Bedner & Ackermann, 2010) die Unterziele Zurechenbarkeit, Authentizität und Revisionsfähigkeit nennen und sich mit Zurechenbarkeit und Authentizität zwei dieser drei Begriffe auch in der Beschreibung von Verbindlichkeit bei Pohl (H. Pohl, 2004) wiederfinden.

Auch Dierstein (Dierstein, 2004) nennt die drei Schutzziele (Dierstein spricht von Dimensionen) Vertraulichkeit, Integrität und Verfügbarkeit und ordnet sie der „Sicht der Verlässlichkeit“ zu. Dabei muss ein verlässliches IT-System „[1.] alle geforderten Aktionen ausführen, [2.] alle nicht geforderten Aktionen zurückweisen und dies [3.] in den geforderten zeitlichen Rahmenbedingungen“ (Dierstein, 2004). Diese Sicht wird durch die komplementäre „Sicht der Beherrschbarkeit“, zu der mindestens die beiden Schutzziele Zurechenbarkeit und Rechtsverbindlichkeit/Revisionssicherheit gehören, ergänzt (Dierstein, 2004). Dabei ist die „Zurechenbarkeit [a]ller Vorgänge und Ergebnisse (Aktionen und Daten) zu definierbaren Veranlassern [… zu] gewährleisten“ und zur Erreichung des Schutzziels Revisionsfähigkeit/Rechtsverbindlichkeit ist die „Beweisbarkeit aller Daten und Vorgänge gegenüber Dritten im Rechtsverkehr [zu] ermöglichen“ (Dierstein, 2004, Tabelle 2). Die beiden Schutzziele der zweiten Sicht finden sich beispielsweise auch bei Pohl (H. Pohl, 2004). Dort wird Revisionssicherheit aufgeführt und mit „Verbindlichkeit“ ein Schutzziel beschrieben, das der Zurechenbarkeit weitestgehend entspricht.

Die zwei Sichten mit ihren insgesamt fünf Schutzzielen nach Dierstein (Dierstein, 2004) sind in Abbildung 1 dargestellt und beschreiben den Begriff IT-Sicherheit. „Fundamental heißen diese Eigenschaften [Schutzziele] auch, weil sie umfassend das

Bedeutungsfeld (Bedeutungsinhalt und Bedeutungsumfang), [also] die Semantik des Begriffs IT-Sicherheit beschreiben“ (Dierstein, 2004). Es muss daher bei einem Sicherheitskonzept oder bei einem Sicherheitsaudit jedes dieser Schutzziele adressiert werden.

Dierstein (Dierstein, 2004) sagt selbst, dass die Schutzziele möglicherweise noch ergänzt werden müssen; den Anspruch der Vollständigkeit erheben sie insbesondere für die Zukunft nicht. Ein mögliches weiteres Schutzziel für die Sicht der Beherrschbarkeit, das heißt der Sicherheit der Betroffenen vor dem System, ist der Datenschutz. Die Definition der Beherrschbarkeit als „Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden“ (Dierstein, 2004), legt dies nahe. Allerdings wird vom Datenschutz selbst wiederum IT-Sicherheit gefordert, sodass die Anforderung des Datenschutzes möglicherweise besser getrennt bleibt. Zudem wird Datenschutz nicht nur hinsichtlich IT-Systemen zu beachten sein, sodass eine Integration in ein IT-Sicherheitskonzept nur einen Teilaspekt darstellen könnte. Dies spricht auch für eine getrennte Betrachtung des Datenschutzes – wie sie in der vorliegenden Arbeit zunächst im 3. Kapitel erfolgt.

Diese Schutzziele haben die Absicht, einen Schaden abzuwenden beziehungsweise die Eintrittswahrscheinlichkeit zu reduzieren (Bedner & Ackermann, 2010). Zusätzlich gibt es Schutzziele, die nicht die Eintrittswahrscheinlichkeit reduzieren wollen, aber als ergänzende vorbeugende Strategie des Risikomanagements das Schadenpotenzial mindern möchten (Hammer, 1999).

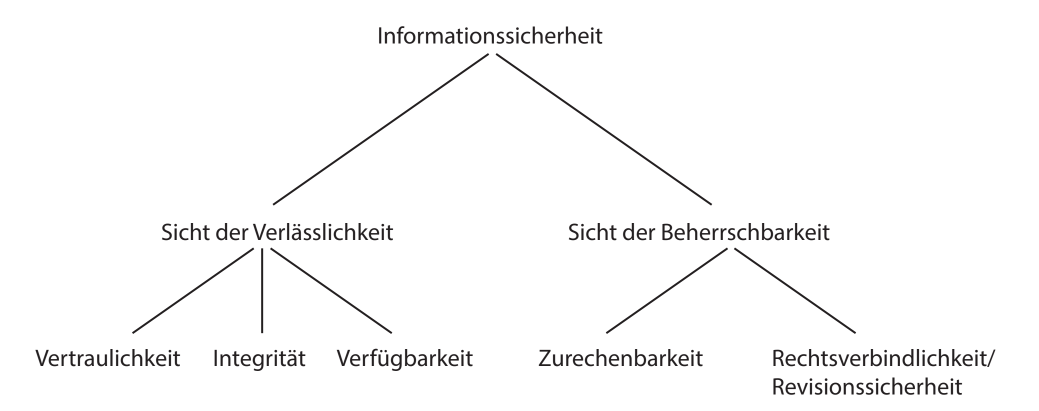


Abbildung 1: Schutzziele der Informationssicherheit

Im Folgenden werden die fünf Schutzziele nach Dierstein (Dierstein, 2004) verwendet, da sie bis auf Kontingenz die Hauptschutzziele der anderen betrachteten Veröffentlichungen umfassen. Kontingenz wurde bewusst nicht ergänzt, da es nicht als für alle Systeme fundamental betrachtet wird.

Informationssicherheit ist durch verschiedene Bedrohungen gefährdet. Nach Pohl (H. Pohl, 2004) lassen sich Bedrohungen nach drei Ursachen unterscheiden:

- höhere Gewalt
- Fahrlässigkeit
- Absichtliches Vorgehen

Nach Grochla u. a. (Grochla, Weber, Albers & Werhahn, 1983) ist als vierte mögliche Ursache noch „technisches Versagen“ zu ergänzen, hierzu gehören beispielsweise Stromausfall und technische Defekte. Der höheren Gewalt ordnen Grochla u. a. (Grochla u. a., 1983) Elementarschadensereignisse (Feuer, Sturm, Erdbeben, Überschwemmungen, aber auch Explosion und Seuchen) sowie Boykotts, Streiks, Aufruhr und Krieg zu.

Das BSI (BSI, 2018) hat 47 „elementare Gefährdungen“ aus „vielen spezifischen Einzelgefährdung[en]“ so herausgearbeitet, dass die Aufzählung kompatibel mit internationalen Gefährdungskatalogen beziehungsweise Sicherheitsstandards ist und jede Gefährdung produktneutral und möglichst auch technikneutral bezeichnet ist. Da eine Gefahr ein „[m]ögliches Eintreten einer Bedrohung gegen ein IT-System“ (H. Pohl, 2004) ist, liegt jeder elementaren Gefährdung eine Bedrohung zugrunde.

Tabelle 1 ordnet die 47 Bedrohungen aus BSI (BSI, 2018, S. 47ff.) den fünf Schutzzielen und vier typischen Ursachen zu. Das bedeutet aber nicht, dass die nicht zugeordneten Ursachen für die jeweilige Bedrohung ausgeschlossen werden können. Auch bei den bedrohten Schutzzielen kann eine indirekte Wirkung auf andere Schutzziele nicht ausgeschlossen werden. So führt beispielsweise ein Stromausfall zunächst zum Absturz eines Datenbankservers (Verfügbarkeit), aufgrund verloren gegangener bestätigter Transitionen (sie waren im Arbeitsspeicher verarbeitet, aber noch nicht persistiert) kann beispielsweise auch die Integrität betroffen sein. Oder das Ausspähen von Informationen dient dem Ausspähen von Zugangsdaten und der nachfolgenden Manipulation von Daten (Integrität) beziehungsweise dem Vornehmen von Handlungen (Verbindlichkeit).

Auch führt ein Verlust der Verfügbarkeit, wenn er nicht durch andere Medien ersetzt werden kann, zu Schwierigkeiten hinsichtlich der Zurechenbarkeit und der Rechtsverbindlichkeit, weil die Daten zum Nachweis fehlen. Auch ist fehlende Integrität ein Problem für die Rechtsverbindlichkeit. Die Schutzziele Zurechenbarkeit und Rechtsverbindlichkeit sind hier jedoch wie alle anderen Schutzziele auch nur markiert, wenn ein Angriff auf das jeweilige Schutzziel direkt bei dieser Bedrohung wahrscheinlich und bei absichtlichen Angriffen beabsichtigt ist.

Tabelle 1: Zuordnung von Bedrohungen zu typischen Ursachen und typischen / primär bedrohten Schutzzielen

elementare Gefahr beziehungsweise Bedrohung	**Ursachen**				**bedrohte Schutzziele**				
	höhere Gewalt	**technisches Versagen**	**Fährlässigkeit**	**absichtliches Vorgehen**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Zurechenbarkeit**	**Rechtsverbindlichkeit**
G01 Feuer	X	X	X	X			X		
G02 ungünstige klimatische Be-dingungen	X		X[3]	X			X		
G03 Wasser	X	X	X	X			X		
G04 Verschmutzung, Staub, Kor-rosion	X	X	X				X		
G05 Naturkatastrophen	X						X		
G06 Katastrophen im Umfeld	X						X		
G07 Großereignisse im Umfeld			X	X			X		
G08 Ausfall oder Störung der Stromversorgung	X	X	X				X		
G09 Ausfall oder Störung von Kommunikationsnetzen	X	X	X			X	X		X
G10 Ausfall oder Störung von Versorgungsnetzen	X	X	X				X		
G11 Ausfall oder Störung von Dienstleistern	X	X	X	X			X		
G12 elektromagnetische Störstrahlung	X	X	X	X		X	X	X	X
G13 Abfangen kompro-mittie-render Strahlung				X	X				
G14 Ausspähen von Informationen (Spionage)				X	X				
G15 Abhören				X	X				

[3] beispielsweise durch das Offenlassen eines Fensters die Wirkung der Klimaanlage (zur Schaffung günstiger Klimabedingungen im Serverraum) zerstören

elementare Gefahr beziehungsweise Bedrohung	**Ursachen**				**bedrohte Schutzziele**				
	höhere Gewalt	**technisches Versagen**	**Fährlässigkeit**	**absichtliches Vorgehen**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Zurechenbarkeit**	**Rechtsverbindlichkeit**
G16 Diebstahl von Geräten, Datenträgern oder Dokumenten				X	X		X		
G17 Verlust von Geräten, Datenträgern oder Dokumenten			X	X	X		X		
G18 Fehlplanung oder fehlende Anpassung[4]			X	X	X	X	X	X	X
G19 Offenlegung schützens-werter Informationen		X	X	X	X				
G20 Informationen oder Produkte aus unzuverlässiger Quelle[5]			X	X		X			
G21 Manipulation von Hard- oder Software				X	X	X	X	X	X
G22 Manipulation von Informationen				X		X			
G23 unbefugtes Eindringen in IT-Systeme				X	X	X	X	X	X
G024 Zerstörung von Geräten oder Datenträgern	X	X	X	X			X		
G25 Ausfall von Geräten oder Systemen		X	X				X		

[4] Das BSI beschreibt die elementare Gefahr wie folgt: „Wenn organisatorische Abläufe, die direkt oder indirekt der Informationsverarbeitung dienen, nicht sachgerecht gestaltet sind, kann dies zu Sicherheitsproblemen führen. Obwohl jeder einzelne Prozessschritt korrekt durchgeführt wird, kommt es oft zu Schäden, weil Prozesse insgesamt fehlerhaft definiert sind […].“ (BSI, 2018, S. 64). Die Gefahr wird durch Abhängigkeiten zwischen Prozessen und fehlerhafter Zuweisung von Verantwortlichkeiten verstärkt.

[5] Das BSI fasst hierunter beispielsweise auch Angriffe mithilfe gefälschter E-Mail-Absender mit dem Ziel, den Empfänger zu falschen Handlungen zu bewegen.

elementare Gefahr beziehungsweise Bedrohung	**Ursachen**				**bedrohte Schutzziele**				
	höhere Gewalt	**technisches Versagen**	**Fährlässigkeit**	**absichtliches Vorgehen**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Zurechenbarkeit**	**Rechtsverbindlichkeit**
G26 Fehlfunktion von Geräten oder Systemen	X	X	X		X	X	X		
G27 Ressourcenmangel	X		X	X			X		
G28 Softwareschwachstellen oder -fehler			X		X	X	X	X	X
G29 Verstoß gegen Gesetze oder Regelungen			X	X	X	X	X		X
G30 unberechtigte Nutzung oder Administration von Geräten und Systemen				X	X	X	X		
G31 fehlerhafte Nutzung oder Administration von Geräten und Systemen			X	X	X	X	X		
G32 Missbrauch von Berechtigungen				X	X	X			
G33 Personalausfall	X		X	X			X		
G34 Anschlag				X			X		
G35 Nötigung, Erpressung oder Korruption				X	X	X	X	X	X
G36 Identitätsdiebstahl				X				X	X
G37 Abstreiten von Handlungen				X				X	
G38 Missbrauch personenbezogener Daten			X	X	X				
G39 Schadprogramme				X	X	X	X	X	X
G40 Verhinderung von Diensten (Denial of Service)				X			X		
G41 Sabotage				X			X		
G42 Social Engineering				X	X				

elementare Gefahr beziehungsweise Bedrohung	**Ursachen**				**bedrohte Schutzziele**				
	höhere Gewalt	**technisches Versagen**	**Fährlässigkeit**	**absichtliches Vorgehen**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**	**Zurechenbarkeit**	**Rechtsverbindlichkeit**
G43 Einspielen von Nachrichten				X	X	X			
G44 unbefugtes Eindringen in Räumlichkeiten	X			X	X	X	X		
G45 Datenverlust	X	X	X	X			X		
G46 Integritätsverlust schützenswerter Informationen		X	X	X		X			
G47 schädliche Seiteneffekte IT-gestützter Angriffe				X	X	X	X	X	X

Später lässt sich mithilfe dieser Tabelle 1 betrachten, welche Bedrohungen durch den in der vorliegenden Arbeit beschriebenen Ansatz adressiert werden.

Mit den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Rechtsverbindlichkeit/Revisionssicherheit sind die unternehmerischen und gesellschaftlichen Ziele beschrieben. Gemäß Biskup (Biskup, 1993) müssen diese durch Ableiten technischer Anforderungen und operationalisierter Maßnahmen konkretisiert werden. In der vorliegenden Arbeit wird nur das Schutzziel der Vertraulichkeit näher betrachtet und daher im nächsten Unterkapitel genauer spezifiziert.

2.2 Vertraulichkeit

Das Schutzziel der Vertraulichkeit wird von Dierstein (Dierstein, 2004) als das älteste Schutzziel der IT-Sicherheit genannt und auch in der ersten Fassung der 1985 veröffentlichen „U.S. Department of Defence Standard Trusted Computer System Evaluation Criteria“ (DoD, 1985) als einziges Schutzziel genannt (auch wenn die anderen Schutzziele damals bereits bekannt waren[6]). Unstreitig ist, dass es als erstes Schutzziel sehr weit entwickelt wurde.

Das Schutzziel der Vertraulichkeit ist, wie im vorherigen Unterkapitel erörtert, Teil der Sicht der Verlässlichkeit. Das heißt, das Schutzziel stammt ursprünglich aus einer Systemperspektive. Soweit jedoch Informationen im Sinne von Nutzdaten und keine Zugangsdaten geschützt werden, sind durch den Schutz der Nutzdaten aber auch die natürlichen und juristischen Personen, denen die Inhalte gehören beziehungsweise auf die sich die Nutzdaten beziehen, geschützt. Dementsprechend ist das Schutzziel nicht trennscharf einer Sicht zuzuordnen, weil es auch Aspekte der Sicht der Beherrschbarkeit als Betroffenenperspektive hat. Die Zuordnung zu einer Perspektive ist aber für die Gewährleistung des Schutzzieles auch nicht entscheidend. Relevanter ist, durch welche Gefahren es bedroht ist. Wie bereits herausgearbeitet, sind dies verschiedene elementare Gefahren[7], sie haben eine ganz unterschiedliche Wirkungsweise. Für den Ansatz dieser Arbeit entscheidend ist, dass etliche einen Bezug zu Geschäftsprozessen haben. So bezieht die Gefahr „Fehlplanung oder fehlende Anpassung“ aus BSI (BSI, 2018) explizit organisatorische Abläufe, Prozesse und Prozessschritte mit ein und kann dementsprechend auch mithilfe von Prozessgestaltung

---

[6] So werden beispielsweise bei Grochla u. a. (Grochla, Weber, Albers & Werhahn, 1983) bereits neben Vertraulichkeit auch Integrität und Verfügbarkeit genannt.

[7] Abfangen kompromittierender Strahlung (G13), Ausspähen von Informationen (Spionage, G14), Abhören (G15), Diebstahl beziehungsweise Verlust von Geräten, Datenträgern oder Dokumenten (G16 beziehungsweise G17), Fehlplanung oder fehlende Anpassung (G18), Offenlegung schützenswerter Informationen (G19), Manipulation von Hard- oder Software (G21), unbefugtes Eindringen in IT-Systeme (G23), Fehlfunktion von Geräten oder Systemen (G26), Softwareschwachstellen oder -fehler (G28), Verstoß gegen Gesetze oder Regelungen (G29), unberechtigte beziehungsweise fehlerhafte Nutzung oder Administration von Geräten und Systemen (G30 beziehungsweise G31), Missbrauch von Berechtigungen (G32), Nötigung, Erpressung oder Korruption (G35), Missbrauch personenbezogener Daten (G38), Schadprogramme (G39), Social Engineering (G42), Einspielen von Nachrichten (G43), unbefugtes Eindringen in Räumlichkeiten (G44), schädliche Seiteneffekte IT-gestützter Angriffe (G47)

abgesichert werden. Es gibt aber auch Gefahren wie das „Abfangen kompromittierender Strahlung“ aus BSI (BSI, 2018), für die der Ansatz dieser Arbeit nicht geeignet ist, weil (primär) technische Maßnahmen oder organisatorische Maßnahmen nicht prozessbezogener Art benötigt werden.

Zunächst muss aber festgelegt werden, was unter dem Schutzziel Vertraulichkeit verstanden wird. Bedner & Ackermann (Bedner & Ackermann, 2010) definieren, dass Vertraulichkeit „bei einem IT-System gewährleistet [ist], wenn die darin enthaltenen Informationen nur Befugten zugänglich sind.“ Nach Eckert (Eckert, 2018, S. 10) gewährleistet ein „System die Informationsvertraulichkeit (engl. confidentiality) […], wenn es keine unautorisierte Informationsgewinnung ermöglicht“. Damit stimmen Definitionen in internationaler Literatur, wie beispielsweise bei Avižienis u. a. (Avižienis, Laprie & Randell, 2004)[8] sowie bei Pfleeger & Pfleeger (Pfleeger & Pfleeger, 2003, S. 10), und Standards, wie ISO 27.000[9], überein, wobei ISO 27.000 konkretisiert, dass die Informationsgewinnung weder durch Personen noch durch Prozesse stattfinden darf. Gemäß Freiling u. a. (Freiling, Grimm, Großpietsch, Keller, Mottok, Münch, Rannenberg & Saglietti, 2014) müssen „vertrauliche Informationen […] vor unbefugter oder unbeabsichtigter Preisgabe geschützt werden“. Im Gegensatz zur Wortwahl von Eckert (Eckert, 2018, S. 10) steht hier nicht die Informationsgewinnung, sondern die Preisgabe im Fokus; während Gewinnung ein Handeln von „außen“ nahelegt, kann Preisgabe auch beispielsweise ein unabsichtliches Handeln von „innen“ umfassen.

Grochla u. a. (Grochla u. a., 1983) unterscheiden zwei unterschiedliche Schutzbereiche mit unterschiedlichen Schutzobjekten. Einerseits soll das **Informationsverhalten** geschützt werden. Hierzu gehören die Metadaten der Kommunikation im

[8] „confidentiality: absence of unauthorized disclosure of information“ (Avižienis, Laprie & Randell, 2004, S. 95)

[9] „confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes“ (International Organization for Standardization, 2014)

Speziellen und der Nutzung der IT im Allgemeinen. Andererseits sollen die **Informationsinhalte** geschützt werden. Im Fokus der vorliegenden Arbeit hinsichtlich Vertraulichkeit steht der Schutz der Informationsinhalte.

Für die vorliegende Arbeit gilt die folgende Definition. Sie basiert auf den obigen Definitionen und betont zudem den Aspekt, dass eine Information nicht ohne Autorisierung von einem Prozess verwendet werden darf.

Definition 2.1:
Informationsvertraulichkeit
Die Anforderung der ***Informationsvertraulichkeit*** *fordert von einem System, dass keine nicht autorisierte (das heißt vom Eigentümer des Systems gewollte) Gewinnung, Offenlegung oder Verwendung von Informationsinhalten durch Personen, Organisationen, Systeme oder Prozesse stattfinden kann beziehungsweise stattfindet.*

Die Informationsinhalte können während ihrer Speicherung und während ihres Transportes durch Verschlüsselung geschützt werden (Bedner & Ackermann, 2010). Dieser Schutzmechanismus ist im Allgemeinen[10] während der Verarbeitung nicht möglich. Der Ansatz der vorliegenden Arbeit möchte daher eine sichere Verarbeitung erreichen.

2.3 Sicherheitsökonomie und Risikomanagement

Absolute IT-Sicherheit, das heißt IT-Sicherheit gegenüber allen bekannten und unbekannten Bedrohungen und in allen praktischen Anwendungsszenarien, kann nicht

[10] Es gibt Ansätze, auf verschlüsselten Daten zu rechnen, sogenannte homomorphe Verschlüsselungsverfahren. Diese sind jedoch in ihren Einsatzmöglichkeiten begrenzt (Wiese, Homann, Waage & Brenner, 2018). Es existieren auch Ansätze, verteilte Datenbanksysteme so zu gestalten, dass Vertraulichkeit zumindest gefördert wird (zum Beispiel Verginadis u. a., 2017).

garantiert werden (vgl. Freiling u. a., 2014; Klein-Hennig & Schmidt, 2017; Merschbacher, 2018). Dies gilt auch im Bereich der Vertraulichkeit. So wird beispielsweise bereits von Shannon (Shannon, 1949) gefordert, dass ein Angreifer mit unbeschränkten Ressourcen (Zeit, Rechenleistung …) aus allem, was er beobachten und analysieren kann, keine Informationen (hier für eine Verschlüsselung über Nachricht oder Schlüssel) gewinnen kann (vgl. Baumann, Franz & Pfitzmann, 2014, S. 76).

Auch wenn es dementsprechend keine absolute Sicherheit gibt, existiert dennoch formal beweisbare Sicherheit. Hierzu müssen das Schutzziel exakt definiert sowie Annahmen über das zugrunde liegende Angreifermodell und das zu schützende System festgelegt werden; innerhalb dieser Grenzen kann es dann beweisbare Sicherheit geben (Baumann u. a., 2014, S. 63). Wegen dieser Abhängigkeit zu den Annahmen sprechen beispielsweise Broadnax u. a. (Broadnax, Mechler, Müller-Quade, Nagel & Rill, 2017) davon, Sicherheit relativ zu definieren. Die mathematische Definition der Sicherheit eines technischen Systems ist schwierig. Mit der spielbasierten Definition und mit der simulationsbasierten Definition gibt es gegenwärtig zwei in der Wissenschaft etablierte Ansätze (Broadnax u. a., 2017).

Schwächer als beweisbare Sicherheit – aber gleichzeitig breiter einzusetzen – ist nachvollziehbare Sicherheit im Sinne von „[f]ormal analysierbare[r] Sicherheit“ und noch schwächer „[i]nhaltlich analysierbare[r] Sicherheit“ (Beutelspacher, 2008, S. 176). Von formal analysierbarer Sicherheit spricht man, wenn man beispielsweise die Sicherheit eines Algorithmus nicht vollständig beweisen, aber „teilweise mathematisch exakt analysieren“ kann. Bei inhaltlich analysierbarer Sicherheit können Argumente für und gegen die Sicherheit eines Verfahrens aufgestellt werden.

Es bleibt die Frage, welches Maß an IT-Sicherheit zu fordern ist. Soll das maximal mögliche Schutzniveau erreicht werden, das heißt jede technische und organisatorische Maßnahme zur Absicherung eines IT-Systems getroffen werden? Da Maßnahmen aber auch immer mit Kosten oder anderen Einschränkungen (beispielsweise bei Bedienbarkeit oder Funktionalität) verbunden sind, ist dies oft (wirtschaftlich) nicht sinnvoll (Grochla u. a., 1983).

Um die Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen zu bewerten, ist es zunächst notwendig, die Kosten eines (möglichen) Sicherheitsvorfalls zu bewerten. Dabei sind Umsatzeinbußen, Wertverlust, Wiederherstellungskosten und Schadensersatzleistungen zu berücksichtigen (Fox, 2011). Anschließend können die Eintrittswahrscheinlichkeit des Schadens und somit das Risiko ermittelt werden. Demgegenüber stehen die Kosten von Sicherheitsmaßnahmen zur Reduktion der Eintrittswahrscheinlichkeit oder der Begrenzung des möglichen Schadens. Diese umfassen Konzeptionskosten, Investitionskosten und Betriebskosten einschließlich Produktivitätsverluste[11] (Fox, 2011). In der Praxis ist es neben der monetären Bewertung schwierig, dass weder Risiken noch Sicherheitsmaßnahmen einzeln vorkommen, sondern immer eine Vielzahl von Fakten betrachtet werden muss. So muss für unterschiedliche Maßnahmenbündel jeweils der Gewinn an Sicherheit (altes Risiko abzüglich neuem Risiko) mit den kumulierten Kosten der Maßnahmen verglichen werden (Fox, 2011).

Die integrierte Modellierung von Anforderungen der Informationsvertraulichkeit in Geschäftsprozessen kann eine ökonomische Betrachtung unterstützen, da die mit den Anforderungen verbundenen Kosten und Einschränkungen (beispielsweise hinsichtlich der Zuweisung von Mitarbeitern) direkt erkennbar oder analysierbar sind.

Die ökonomische Sicherheit ist nicht immer möglich. Drei typische Gründe für weiterführende Sicherheitsmaßnahmen sind die Erfüllung gesetzlicher Verpflichtungen, gesellschaftliche Erwartungen und/oder eigene ethische Prinzipien der beteiligten Personen.

- Gesetz: Unabhängig von der Wirtschaftlichkeit von Schutzmaßnahmen können diese zur Erfüllung gesetzlicher Anforderungen notwendig sein. Darauf weisen bereits Grochla u. a. (Grochla, Weber, Albers & Werhahn, 1983) hin.

[11] Insofern ist auch eine möglicherweise aufwendigere Bedienung hier bereits berücksichtigt. Dabei kann auch berücksichtigt werden, dass aufgrund einer Sensibilisierung die Bereitschaft, Einschränkungen der Benutzerfreundlichkeit hinzunehmen, steigt (Grochla u. a., 1983). Es muss dennoch beachtet werden, dass eine signifikant schlechtere Benutzerfreundlichkeit zur Umgehung mittels Schatten-IT und somit zu neuen Sicherheitsrisiken führen kann.

Mögliche Beispiele solcher Gesetze sind je nach Anwendungsfall das Datenschutzrecht oder bei kritischen Infrastrukturen das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).

- Gesellschaft: Für bestimmte Szenarien erwartet die Gesellschaft ein bestimmtes Schutzniveau, die Nichtbeachtung dieser Erwartungshaltung kann bei Bekanntwerden beispielsweise zu Wettbewerbsnachteilen führen.
- Ethik: Eine Organisation muss beziehungsweise möchte sich, sofern vorhanden, auch an eigene ethische Leitlinien beziehungsweise Verhaltenskodizes halten[12]. Zudem haben beteiligte Personen eigene ethische Vorstellungen, die sie im Rahmen ihrer Möglichkeiten in die Entscheidungsfindung beziehungsweise Wahrnehmung ihrer Aufgaben einbringen. Ethische Zusatzanforderungen können sich daraus dann konkret unter anderem durch mögliche Schäden ergeben, die unabhängig von ihrer wirtschaftlichen Bedeutung nicht akzeptabel sind und daher durch besondere Maßnahmen so weit wie möglich ausgeschlossen werden müssen. Eine andere Ursache sind mögliche Schäden, die materiell nicht oder zu niedrig erfasst werden, aber aus Sicht der Beteiligten eine höhere Bedeutung haben. Die Zusammenhänge von Ethik und Sicherheit wurden seit 2016 auch im Rahmen des EU-Forschungsprogrammes Horizon 2020 als Koordinations- und Unterstützungsaktivität „Constructing an Alliance for Value-driven Cybersecurity“ (CANVAS) untersucht[13]. Im Rahmen des Projektes ist auch eine Literaturstudie (Yaghmaei u. a., 2017) entstanden, welche gezeigt hat, dass ethische Fragen der Informationssicherheit gegenwärtig nicht etabliert sind, sondern dass sich die Ethikforschung rund um die Informationsverarbeitung auf andere Themen wie Big Data und Datenschutz konzentriert.

[12] Beispielsweise hat das KIT ethische Leitlinien öffentlich unter https://www.kit.edu/downloads/KIT_Ethische_Leitlinien.pdf publiziert.

[13] https://canvas-project.eu

Es ist daher zielführender, von einem angemessenen Sicherheitsniveau zu sprechen – dieses kann dann alle Gesichtspunkte umfassen. Zudem ist es wichtig, nicht nur einen Teil eines IT-Systems zu betrachten, sondern Informationssicherheit möglichst ganzheitlich zu sehen.

3 Grundlagen: Datenschutz

Datenschutz bezeichnet den Schutz personenbezogener Daten zur Einhaltung des Grundrechts auf informationelle Selbstbestimmung aller natürlichen Personen (vgl. Gola, Jaspers, Müthlein & Schwartmann, 2016), dementsprechend wird der Datenschutz auch als „Garant" des Grundrechts auf informationelle Selbstbestimmung bezeichnet (so beispielsweise in Voßhoff, 2015). Der Schutz personenbezogener Daten ist abzugrenzen vom Schutz anderer Daten. So schreibt der ehemalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar: „[B]eim Datenschutz geht es nicht um den Schutz von Daten schlechthin, sondern um den Schutz personenbezogener Daten, und zwar vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung und der Gewährleistung der Privatsphäre." (Schaar, 2017a, S. 23)

Im ersten Abschnitt dieses Kapitels wird die Geschichte des Datenschutzes kurz zusammengefasst, um später verschiedene Begriffe besser einordnen zu können, bevor im zweiten Abschnitt die Bedeutung des Datenschutzes für die Gesellschaft und für Einzelpersonen erklärt wird. Damit wird motiviert, warum Datenschutz relevant ist, und warum sich Unternehmen, die sich rechtstreu verhalten wollen beziehungsweise aus anderen beispielsweise moralischen Gründen die informationelle Selbstbestimmung ihrer Kunden oder deren Daten schützen wollen, sich um Datenschutz systematisch sorgen müssen. Da für alle Unternehmen, sofern sie den europäischen Markt adressieren und personenbezogene Daten verarbeiten, die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) als aktuell wichtigste Datenschutznorm relevant ist, wird im dritten Abschnitt ihr sachlicher und räumlicher Anwendungsbereich beschrieben. Zuletzt werden im vierten Abschnitt die neun Grundsätze der EU-DS-GVO erläutert. Dabei werden ausgewählte Grundsätze, die mithilfe des Ansatzes dieser Arbeit umgesetzt werden können, detaillierter beschrieben.

3.1 Geschichte des Datenschutzrechtes

Damit später verwendete Begriffe besser eingeordnet und in ihrer – durch die Historie mitbestimmten Bedeutung – erfasst werden können, erfolgt zunächst eine Einführung in die (junge) Geschichte des Datenschutzrechtes. Dies ist auch deswegen von Bedeutung, weil die neue Europäische Datenschutz-Grundverordnung aufgrund ihrer Neuheit und der folglich fehlenden höchstrichterlichen Urteile Interpretationsspielraum bietet, der so ggf. reduziert werden kann.

Aufgrund der „Entstehung großer Rechenzentren entstand Ende der sechziger Jahre […] die Notwendigkeit, den Bürger vor Missbrauch der Vielzahl über ihn nun speicherbaren Daten […] zu schützen.“ (Scholz, 2017, Rn. 9). Damals stand der Schutz des Bürgers vor staatlichem Handeln im Fokus, weil der Staat beziehungsweise die Behörden begannen, große Rechenzentren aufzubauen. Das weltweit erste Datenschutzgesetz ist 1970 in Hessen in Kraft getreten (Leeb & Liebhaber, 2018, S. 534). Es folgten Landesdatenschutzgesetze in weiteren Bundesländern (beispielsweise Rheinland-Pfalz 1974, Bayern 1978, Schleswig-Holstein 1978, Baden-Württemberg 1979, Hamburg 1981). Hierdurch war jedoch nur das Handeln durch Landesbehörden geregelt, das Handeln von Bundesbehörden wurde erstmals 1977 durch das Bundesdatenschutzgesetz geregelt (Scholz, 2017, Rn. 9). Auch in anderen Staaten wurden Gesetze zum Umgang mit personenbezogenen Daten erlassen, so beispielsweise 1974 in den USA mit dem „Privacy Act“ (Leeb & Liebhaber, 2018, S. 535). Auch wenn es mit diesen Gesetzen für ihren jeweiligen Geltungsbereich erstmals allgemeine Regelungen zum Datenschutz gab, ist das Interesse dahinter keineswegs neu gewesen. So schreibt die erste Landesbeauftragte für den Datenschutz des Landes Baden-Württemberg, Dr. Ruth Leuze, in ihrem ersten Tätigkeitsbericht: „Ziel des Datenschutzes ist, in unserer hoch entwickelten Informationsgesellschaft den Mißbrauch persönlicher Daten zu verhindern. […] Datenschutz ist keine Modeerscheinung. Gewiß, die Terminologie ist neu. Seine Zielsetzung aber ist unserer Rechtsordnung – wenn auch nicht in voller Breite – seit langem vertraut. Zu ihrer Tradition gehören eine Vielzahl datenschutzrechtlicher Regelungen. Ich denke zum Beispiel an das Arzt-, Steuer-,

Bank- und Postgeheimnis […].“ (Leuze, 1980, S. 7) Dass Datenschutz keine Modeerscheinung war, kann über 30 Jahre nach dem Bericht beispielsweise durch die große gesellschaftliche Auseinandersetzung damit bestätigt werden. Bereits in diesen Gesetzen waren die Grundsätze der Erforderlichkeit, der Sicherheit und der Transparenz enthalten (Leeb & Liebhaber, 2018, S. 535).

Die Datenschutzgesetze wurden aufgrund des Volkszählungsurteils 1983 und der öffentlichen Diskussion nochmals vollständig überarbeitet, sodass 1990 ein neues Bundesdatenschutzgesetz verabschiedet wurde (Hornung & Schnabel, 2009). Das Bundesverfassungsgericht hatte früh das „Allgemeine Persönlichkeitsrecht“ aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes (GG) abgeleitet; es lässt sich in die drei Schutzbereiche Selbstbewahrung, Selbstdarstellung und Selbstbestimmung untergliedern (Martini, 2009). Das allgemeine Persönlichkeitsrecht beruht auf dem Recht zur freien Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) und auf der Menschenwürde (Art. 1 Abs. 1 GG) und steht jeder Person zu. Die beiden Artikel des Grundgesetzes, aus denen dieses Recht abgeleitet ist, sind seit ihrer Bekanntgabe am 23.05.1949 unverändert im Wortlaut:

- „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“ (Artikel 1 Absatz 1 Grundgesetz)
- „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“ (Artikel 2 Absatz 1 Grundgesetz)

Aus dem Allgemeinen Persönlichkeitsrecht hat das Bundesverfassungsgericht 1983 das Grundrecht auf informationelle Selbstbestimmung geschöpft[1]. Es wird dem Schutzbereich Selbstbestimmung des Allgemeinen Persönlichkeitsrechts zugeordnet. Die Beschwerdeführer der dem Urteil zugrunde liegenden Verfassungsbeschwerden

[1] Dies bedeutet, dass das Grundrecht nicht wortwörtlich im Grundgesetz enthalten ist, aber nach Rechtsprechung des Bundesverfassungsgerichtes aus dem Text abgeleitet werden kann.

im Speziellen und die Gesellschaft im Allgemeinen hatten befürchtet, dass die Volkszählung „die Grundlage für eine schrankenlose, durch die automatisierte Verarbeitung begünstigte Verknüpfung der unzähligen, von den verschiedensten staatlichen und privaten Stellen bereits gespeicherten Daten abgeben könnte“ (Simitis, 2014, Rn. 28). Das Bundesverfassungsgericht hat diese Furcht ernst genommen und sich über den korrekten Sachverhalt der Volkszählung hinaus ausführlich damit auseinandergesetzt, welche Anforderungen das Grundgesetz an die Erhebung, Speicherung und Verarbeitung personenbezogener Daten stellt (Simitis, 2014, Rn. 29). Das Volkszählungsurteil ist daher auch für den heutigen Datenschutz noch von Bedeutung. Simitis (Simitis, 2014) hat acht Vorgaben für den Datenschutz aus dem Urteil vom 15.12.1983 extrahiert:

1. „Die Zulässigkeit der Verarbeitung ist […] eine verfassungsrechtliche Frage“ (Rn. 30).
2. Die Entscheidung, ob und in welchem Umfang Daten einer Person gespeichert werden dürfen, muss zunächst der Person überlassen bleiben (Rn. 31). Diese informationelle Selbstbestimmung schließt das Recht ein, die Verarbeitung einzuschränken beziehungsweise zu untersagen, aber eben auch, sie zu erlauben.
3. Die informationelle Selbstbestimmung ist nicht uneingeschränkt gewährleistet, sie hat jedoch Priorität. Das bedeutet, dass der Einzelne nur „ausnahmsweise übergangen werden darf, […] lediglich in den Fällen, in denen ein ‚überwiegendes Allgemeininteresse‘ für eine Verarbeitung spricht“ (Rn. 33).
4. Einschränkungen der informationellen Selbstbestimmung, das heißt das Übergehen des Einzelnen (vgl. Punkt 3), sind für konkrete Anwendungen nur durch Gesetz möglich (Rn. 32).
5. Das Kriterium für den Datenschutz ist die Personenbezogenheit – nicht die Art der Angaben (Rn. 34).
6. Daten unterliegen einer strengen Zweckbindung, damit der Betroffene vor seiner Einwilligung beziehungsweise der Gesetzgeber vor Verabschiedung

des Gesetzes sich möglichst zuverlässig ein Bild von den möglichen Folgen der Verarbeitung machen können (Rn. 35).

7. Eine Zweckentfremdung darf auch bei Weitergabe der Daten nicht stattfinden. Ebenso innerhalb der Verwaltung muss der „Gesetzgeber […] deshalb für einen ‚amtshilfefesten Schutz gegen die Zweckentfremdung' sorgen" (Rn. 36).
8. Da weder die betroffene Person noch der Gesetzgeber (je nachdem, ob die Verarbeitung aufgrund einer informationellen Selbstbestimmung oder eines Gesetzes erfolgt) in der Lage ist, die technologische Weiterentwicklung immer zu verfolgen und dies durch die Komplexität der Verarbeitung bei sich regelmäßig verändernden Methoden weiter erschwert wird, ist die Kontrolle mittels einer „eigens dafür eingerichtete[n] Instanz" vorgeschrieben. Diese unabhängige Instanz, der Datenschutzbeauftragte, soll zudem die Transparenz erhöhen.

Das Volkszählungsurteil des Bundesverfassungsgerichtes ist folglich unter anderem bedeutsam, weil das so geschöpfte Grundrecht informationelle Selbstbestimmung den dazu notwendigen Datenschutz in der Verfassung verankert und den bisherigen Datenschutz um das neue Prinzip der Zweckbindung ergänzt.

Auch innerhalb Europas hat der Datenschutz bereits eine längere Geschichte. Gola (Gola, 2018, Rn. 6) beschreibt den Artikel 8 der Europäischen Menschenrechtskonvention vom 4. November 1950 als erste europäische verfassungsmäßige Bestimmung mit Datenschutzbezug. Die Europäische Menschenrechtskonvention wurde nach und nach von allen 47 Mitgliedsstaaten (darunter auch alle EU-Mitglieder) ratifiziert (Selmayr & Ehmann, 2017, Rn. 10). Artikel 8 bestimmt u. a. die Achtung des Privatlebens, der Wohnung und der Kommunikation. Der Artikel 8 basiert seinerseits wiederum auf Artikel 12 der Menschenrechtserklärung der Vereinten Nationen vom 10. Dezember 1948. Der Europarat[2] hat ebenfalls verschiedene Übereinkommen zum

[2] Der Europarat ist kein Organ der Europäischen Union und daher nicht mit dem Europäischen Rat zu verwechseln. Er ist vielmehr ein von der Europäischen Union unabhängiger Zusammenschluss europäischer Staaten. Ihm gehört beispielsweise auch die Schweiz an.

Datenschutz geschlossen. Nach Gola (Gola, 2018, Rn. 8) ist das bedeutsamste und von allen Mitgliedsstaaten ratifizierte das „Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten“ von 1981. Dabei ging es nicht nur darum, ein festgelegtes Maß an Datenschutz in allen Mitgliedsstaaten, sondern auch den freien Datenverkehr sicherzustellen (Selmayr & Ehmann, 2017, Rn. 12). So heißt es in Artikel 12 Absatz 2 des Übereinkommens: „Eine Vertragspartei darf allein zum Zweck des Schutzes des Persönlichkeitsbereichs den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen.“

Die Europäische Union hat in der Charta der Grundrechte der Europäischen Union (in Kraft getreten am 1. Dezember 2009 zusammen mit dem Vertrag von Lissabon) ebenfalls den Schutz personenbezogener Daten in primärem EU-Recht verankert. Zunächst ist Artikel 7 Absatz 1 fast wortgleich wie Artikel 8 Absatz 1 der Europäischen Menschenrechtskonvention von 1950. Artikel 8 der Charta der Grundrechte der Europäischen Union bestimmt dann:

„Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten, legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“
Charta der Grundrechte der Europäischen Union, Fassung von 2016 (2016/C 202/02)

Im europäischen Sekundärrecht gab es bereits früher Regelungen zur Harmonisierung des Datenschutzrechtes in Europa. Dies geschah zunächst durch zwei Richtlinien:

- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie)
- Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – ePrivacy-Richtlinie)

Diese galten beziehungsweise gelten (wie alle Richtlinien der EU) nicht unmittelbar in allen Mitgliedsstaaten, sondern sie müssen von diesen noch in nationales Recht umgesetzt werden. In Deutschland wurde beispielsweise das BDSG entsprechend angepasst. Da die Richtlinien nicht unmittelbar gelten und einige Mitgliedstaaten sehr große Spielräume bezüglich der Umsetzung sahen und auch nutzten, wurde ein einheitliches europäisches Datenschutzniveau damit nicht erreicht (Gola, 2018, Rn. 13). Dies ist eine der Ursachen für die Reform des europäischen Datenschutzes mithilfe einer Verordnung, das heißt mithilfe von unmittelbar in allen EU-Mitgliedsstaaten geltendem Recht. Eine Verordnung darf durch die Mitgliedsstaaten nicht modifiziert werden, jedoch gibt es die Möglichkeit, den Mitgliedsstaaten durch Öffnungsklauseln definierte Gestaltungsspielräume für nationales Recht zu schaffen (Wolf, 2017, Rn. 218–221).

Auch bei dieser Reform wurden wie bei dem Übereinkommen des Europarates von 1981 und der Datenschutzrichtlinie der EU von 1995 zwei Zielsetzungen verfolgt (Selmayr & Ehmann, 2017, Rn. 18). So heißt es bereits in einer Mitteilung der Europäischen Kommission an das Europäische Parlament, den Europäischen Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 4. November 2010 bezüglich eines Gesamtkonzeptes für den Datenschutz in der Europäischen Union: „Die Datenschutzrichtlinie von 1995 war ein Meilenstein in der

Entwicklung der Datenschutzpolitik der Europäischen Union. Die Richtlinie bestätigt zwei der ältesten, gleichermaßen wichtigen Ziele des europäischen Integrationsprozesses: Einerseits den Schutz der Grundrechte und der Grundfreiheiten des Einzelnen, insbesondere des Grundrechts auf Datenschutz, und andererseits die Vollendung des Binnenmarktes – in diesem Fall den freien Verkehr personenbezogener Daten. Diese beiden Ziele sowie die Grundsätze der Richtlinie gelten fünfzehn Jahre später unverändert.“ (Europäische Kommission, 2010)

Die EU-Kommission hat 2012 einen Vorschlag vorgelegt, der diesen beiden Zielen, das heißt dem Datenschutz und dem freien Datenverkehr innerhalb der EU, dient (Gola, 2018, Rn. 14+17). In den folgenden Jahren haben das Europäische Parlament und der Europäische Rat sich eigenständig damit auseinandergesetzt und Vorschläge erarbeitet. Im Rahmen eines 2015 begonnenen Trilogs einigten sich das Europäische Parlament, der Europäische Rat und die EU-Kommission dann auf einen gemeinsamen Entwurf. Schließlich wurde am 14. April 2016 die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ vom Europäischen Parlament verabschiedet. Sie ist am 25. Mai 2016 in Kraft getreten und seit dem 25. Mai 2018 (nach einer Vorbereitungszeit von 2 Jahren) gültig (Gola, 2018, Rn. 18+19). Die EU-DS-GVO besteht aus 99 Artikeln und 173 Erwägungsgründen[3].

Eine wesentliche Neuerung ist die verbesserte Durchsetzung eines durch die EU-DS-GVO, abgesehen von nationalen Gestaltungsspielräumen aufgrund der Öffnungsklauseln, nun einheitlich für die ganze Europäische Union festgelegten Datenschutzrechtes (Selmayr & Ehmann, 2017, Rn. 60). Die Durchsetzung wird beispielsweise aufgrund des nun festgelegten Marktortprinzips, der Schaffung eines europäischen

[3] Erwägungsgründe sind nicht selbst Verordnung – aber sie sind bei der Auslegung der Verordnung zu berücksichtigen.

Datenschutzausschusses und signifikant gestiegener Sanktionsmöglichkeiten bei Datenschutzverstößen verbessert (Selmayr & Ehmann, 2017, Rn. 68-74). Dazu kommen neue Regelungen wie das Recht auf Datenübertragbarkeit beziehungsweise Datenportabilität (Art. 20 EU-DS-GVO), das Koppelungsverbot (Art. 7 Abs. 4 EU-DS-GVO) und die Rechenschaftspflicht (Art. 5 Abs. 2 EU-DS-GVO) (Selmayr & Ehmann, 2017, Rn. 64-66). Außerdem gibt es weiterentwickelte Regeln: So wurde der bisherige Löschanspruch zum Recht auf Vergessenwerden (Art. 17 EU-DS-GVO) weiterentwickelt (Selmayr & Ehmann, 2017, Rn. 63).

Die neue europäische Datenschutz-Grundverordnung hat notwendigerweise auch zu einem durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) neu gefassten Bundesdatenschutzgesetz geführt. Auch weitere Gesetze wie beispielsweise Landesdatenschutzgesetze der Bundesländer oder kirchliche Datenschutzgesetze wurden angepasst (Kugelmann, 2018; Hoeren, 2018).

Die Richtlinie 2002/58/EG – ePrivacy-Richtlinie – ist gegenwärtig weiter gültig. Sie soll zusammen mit der Richtlinie 2009/136/EG – Cookie-Richtlinie – durch eine ePrivacy-Verordnung abgelöst werden. Die Trilog-Verhandlungen sollen nach Piltz (Piltz, 2018) im 2. Halbjahr 2018 beginnen. Das bayerische Landesamt für Datenschutzaufsicht hat eine Synopse der Vorschläge der EU-Kommission und des Europäischen Parlamentes veröffentlicht und wird diese um den Vorschlag des Europäischen Rates – sobald verfügbar – ergänzen (Bayerisches Landesamt für Datenschutzaufsicht, 2018). Die ePrivacy-Verordnung soll „die besonderen Fragen des Datenschutzes bei der Verarbeitung elektronischer Kommunikations(meta-)daten im Zuge der Nutzung elektronischer Kommunikationsdienste regeln." (Piltz, 2018) Nach den aktuellen Vorschlägen soll dabei auch der Datenschutz durch IP-basierte Dienste (Over-the-top-Dienste) und webbasierte E-Mail-Dienste geregelt werden. Damit „soll ein wirksamer und einheitlicher Schutz der Endnutzer bei der Benutzung funktional gleichwertiger Dienste gewährleistet werden", so der Entwurf des Europäischen

Parlaments vom 23.10.2017 (zitiert nach Bayerisches Landesamt für Datenschutzaufsicht, 2018). Die ePrivacy-Verordnung soll zusammen mit der EU-DS-GVO gelten und wird zu einer Anpassung oder Abschaffung des Telemediengesetzes in Deutschland führen.

3.2 Bedeutung des Datenschutzes

Bereits im Volkszählungsurteil von 1983 heißt es, dass das Recht auf informationelle Selbstbestimmung notwendig sei, da sonst „nicht nur die individuellen Entfaltungschancen des Einzelnen [beeinträchtigt würden], sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“ (BVerfG, 1984, S. 43) Wenn das Grundrecht nicht gewährleistet sei, müsse der Bürger damit rechnen, dass das eigene Verhalten jederzeit erfasst, dauerhaft gespeichert, analysiert, verwendet und/oder weitergegeben wird; dementsprechend würde der Bürger sein Verhalten anpassen (BVerfG, 1984, S. 43). Durch Verknüpfen beziehungsweise Zusammenführen unterschiedlicher Datenbestände wird das Problem noch verstärkt. Das Recht auf informationelle Selbstbestimmung ist also ein für das Funktionieren unserer Demokratie notwendiges Grundrecht, und Datenschutz ist entsprechend auch notwendig, um eine freiheitliche Demokratie zu gewährleisten.

Auch wenn die Gefahr der Erfassung, Speicherung, Analyse, Verwendung und Weitergabe des Verhaltens bereits im Volkszählungsurteil von 1983 beschrieben ist, so ist diese Gefahr heute noch akuter. Zu staatlichen Akteuren kommen privatwirtschaftliche Akteure hinzu. So gehört es zum Geschäftsmodell von Konzernen wie Facebook und Google, Daten von Nutzern zu erfassen und diese zu analysieren, um den Nutzer besser zu kennen und dann dieses Wissen durch den Verkauf von individualisierter

Werbung zu monetarisieren (Kübler, 2018). Der Datenbestand wird aber nicht nur privatwirtschaftlich genutzt. Spätestens seit den PRISM-Enthüllungen durch Edward Snowden sei klar, „dass auch staatliche Stellen, insbesondere aus dem Kreis der Sicherheitsbehörden, an den enormen privatwirtschaftlich angehäuften Informations- und Datenschätzen partizipieren." (Leutheusser-Schnarrenberger, 2017, S. 123). Eine Gefährdung der Demokratie entstünde aber nicht nur durch angepasstes Verhalten von Bürgern, sondern auch durch die „grundsätzliche Umgestaltung der Zivilgesellschaft, der Wirtschaftssysteme und damit auch der Einflussmöglichkeiten der Politik durch die Digitalisierung" (Leutheusser-Schnarrenberger, 2017, S. 125). Das Recht auf informationelle Selbstbestimmung und der dazu notwendige Datenschutz können einen Beitrag leisten, die Gefährdung der Demokratie zu verringern.

Es ist jedoch nicht nur die Funktionstüchtigkeit der Demokratie bedroht, mangelnder Datenschutz führt auch zu Nachteilen für den Einzelnen. Denn aktuelle und künftige Big-Data-Methoden können mit zunehmender Menge an verfügbaren Daten das menschliche Verhalten besser darstellen und genauer beziehungsweise zuverlässiger vorhersagen (Schaar, 2017b). Die Nachteile entstehen beispielsweise konkret durch Scoring-Verfahren, das heißt Verfahren zur Bewertung einer einzelnen Person, ggf. bezogen auf eine Vergleichsgruppe oder Gesamtheit, unter Nutzung von Big Data. Durch zunehmende Möglichkeiten der Auswertung von Big Data und der Erschließung von weiteren Datenquellen „werden immer mehr Lebensbereiche durch Score-Werte durchdrungen und bestimmen damit die rechtsgeschäftlichen Möglichkeiten der Betroffenen" (Eschholz, 2017). Ein typischer Anwendungsfall von Scoring-Verfahren ist die Ermittlung der Kreditwürdigkeit. Die SCHUFA wollte bereits 2012 zusammen mit dem HPI untersuchen, wie Daten aus sozialen Netzwerken für die Berechnung des SCHUFA-Score genutzt werden könnten, hat es aber aufgrund öffentlichen Drucks unterlassen (Eschholz, 2017). Facebook besitzt jedoch bereits ein Patent, welches unter anderem die Verwendung von Daten aus sozialen Netzwerken und insbesondere die Information über dortige Beziehungen für Kreditentscheidungen nutzt (US9798777B2, 2017, Absatz 10). Auch andere ausländische Unternehmen wie beispielsweise Kreditech setzen Daten aus sozialen Netzwerken ein (Huch,

2016). Ein weiterer Anwendungsfall ist unter Einbeziehung von Datenquellen aus Fitness-, Verhaltens- und Gesundheitssensoren die Risikoermittlung für private Krankenversicherungen (Stach u. a., 2018).

Datenbestände können auch zur Preisdiskriminierung eingesetzt werden. Preise können dann individualisiert werden. Durch Big Data stehen neben bisherigen Ansätzen wie Preisdiskriminierung nach Zeit, Ort, Vertriebskanal und ggf. Rabattgruppe (Studierendenrabatt) weitere Datenquellen zur Verfügung, um die individuelle Zahlungsbereitschaft eines Interessenten möglichst vollständig auszuschöpfen (Schleusener, 2017).

Dabei stehen technisch immer mehr Daten zur Verfügung, weil in vielen Lebensbereichen manuelle Systeme durch automatisierte/rechnergestützte Systeme ersetzt werden (Schaar, 2017b). Diese elektronischen Systeme sind in vielen Fällen vernetzt, der Begriff „Internet der Dinge“ ist zum Schlagwort hierfür geworden. Selbst ein Bürger, welcher auf soziale Netzwerke wie Facebook, Twitter, Instagram, Xing und viele mehr verzichtet und Messenger wie WhatsApp nicht einsetzt, wird so durch zunehmend mehr Stellen digital erfasst. Selbst durch einen Verzicht auf Smartphone, Notebook und Internet würde sich dieser Bürger aufgrund elektronischer Ticketautomaten, digitaler Kassensysteme und Zahlungswege, intelligenter Autos und smarter Fernseher laut Schaar (Schaar, 2017b) der Erfassung von Daten über sich nicht entziehen können. Selbst wenn man diese Ansicht nicht teilt, ist klar, dass über die meisten Personen aufgrund der fortschreitenden Digitalisierung und der eigenen Lebensgewohnheiten (Nutzung von Smartphone und Kreditkarte, Nutzung von Rabattsystemen, Nutzung von digitalen Plattformen wie Amazon, eBay, AirBnB …) viele Daten technisch erfassbar sind. Hinzu kommt die weitere Verschiebung der Machtverhältnisse aufgrund von Lock-in-Effekten. Im Gegensatz zu normalem Telefon, World Wide Web, SMS oder klassischen E-Mails mit offenen Standards setzten neue Messengerdienste wie WhatsApp oder soziale Netzwerke wie Facebook oder LinkedIn auf geschlossene Systeme. Der Nutzer solcher Dienste hat einen Anreiz, selbst möglichst Dienste mit großen Netzwerken zu nutzen, da sein individueller Nutzen

dadurch steigt (Schaar, 2017b). Bei späteren Wechseln wird der Effekt noch dadurch verstärkt, dass der Nutzer erneut seine digitalen Freundschaftsbeziehungen (Freunde, Follower …) aufbauen muss beziehungsweise seine alten Freundschaftsbeziehungen überreden muss, zusammen mit ihm umzuziehen. In der Praxis muss ein Nutzer, der einen geschlossenen Messenger wechseln möchte, seine Freunde überzeugen, den neuen Messenger auch einzusetzen oder auf den jeweiligen Kommunikationskanal oder gar den ganzen Kontakt zu verzichten. Dieser Lock-in-Effekt[4] verstärkt die Kundenbindung und „ermöglicht es den Unternehmen [Anbietern], den Mitgliedern [Nutzern] einseitig die Bedingungen zu diktieren, unter denen ihre Daten verarbeitet und ausgewertet werden" (Schaar, 2017b, S. 109). Unter diesen Umständen ist ein effektiver Verbraucherdatenschutz schwer zu gewährleisten, weil sich Anbieter vielfach auf die erteilten Einwilligungen berufen.

Dadurch nimmt die Datenbasis für Big-Data-Analysen weiter zu. 2014 betrug laut Hilbert (Hilbert, 2015) die weltweite Speicherkapazität 4,6 Zettabytes[5] und ist seit 1986 jährlich um durchschnittlich 31 % gewachsen. 2002 waren gemäß der Studie erstmals mehr mediatisierte Informationen digital gespeichert als analog verfügbar waren, 2014 wurden nur noch 0,5 Prozent der neu erzeugten mediatisierten Informationen ausschließlich analog gespeichert. Hinzu kommt, dass auf digitale Informationen in vielen Fällen aufgrund vernetzter Infrastrukturen unabhängig von Zeit und Raum zugegriffen werden kann (Schaar, 2017b).

Auch aufgrund der fortschreitenden Digitalisierung und der scheinbar unbegrenzten Speichermöglichkeiten ist das Grundrecht auf informationelle Selbstbestimmung und daher auch das Instrument des Datenschutzes also wie dargestellt sowohl für eine freiheitliche, demokratische Gesellschaft als auch für den Einzelnen notwendig.

[4] Der Lock-in-Effekt wird auch noch durch weitere Aspekte verstärkt. Dazu gehört beispielsweise das bisherige Kommunikationsarchiv in Messengersystemen oder die bereits erstellten Beiträge, Bildergalerien usw. in sozialen Netzwerken.

[5] 1 Zettabyte = 10^{21} Bytes

Unabhängig von anderen aktuell diskutierten Instrumenten, um nachteilige Effekte durch mangelnden Datenschutz beziehungsweise große Datenmacht auszugleichen (beispielsweise „Zugang zum ‚Datenschatz' nach der Essential-facilities-Doktrin" (Körber, 2016, S. 96)), muss auch der Datenschutz weiterentwickelt beziehungsweise durchgesetzt werden, da er ebenfalls ein wichtiges und aktuell auch das am weitesten entwickelte Instrument darstellt.

Nach Bizer (Bizer, 2007) kann und muss der Staat seiner Schutzpflicht hinsichtlich des Datenschutzes durch vier Säulen nachkommen.

1. Datenschutz durch Recht
2. Datenschutz durch Technik
3. Datenschutz als Wettbewerbsfaktor
4. Datenschutz durch Prozessmanagement

Dabei stehen ihm unterschiedliche Instrumente von der Gesetzgebung bis hin zu Fördermaßnahmen zur Verfügung. Ein Beispiel für Datenschutz durch Technik ist das durch die Baden-Württemberg-Stiftung finanzierte Projekt „Anwendung zur Verteilung und Auswahl rechtskonformer Datenschutzeinstellungen" (AVARE). Dabei wurde mithilfe aktueller technischer Möglichkeiten unter Beachtung des derzeitigen Rechtsrahmens (Alpers, Pieper & Wagner, 2017) eine Lösung zur informationellen Selbstbestimmung für Bürger (Alpers, Oberweis, u. a., 2017) geschaffen. Die vorliegende Arbeit versteht sich dagegen als Beitrag zur vierten Säule „Datenschutz durch Prozessmanagement".

Auch weil der Staat seine Schutzpflicht weiter wahrnehmen wird und beispielsweise mit der EU-DS-GVO gerade den Datenschutz weiter gestärkt hat, muss es im Interesse der Unternehmen sein, Datenschutz zu beachten. Dabei gilt es, die Chancen von Big Data beziehungsweise einer intelligenten Datenverarbeitung unter Einhaltung der Datenschutzbestimmungen und insbesondere des Rechtes auf informationelle Selbstbestimmung zu nutzen. Diese Arbeit möchte hierzu durch Bereitstellen neuer Ansätze einen Beitrag leisten.

3.3 Anwendungsbereich EU-DS-GVO

Der Anwendungsbereich muss einerseits sachlich (Wer ist geschützt? Was ist geschützt?) nach Artikel 2 EU-DS-GVO und andererseits räumlich (Wo gilt der Schutz?) nach Artikel 3 EU-DS-GVO abgegrenzt werden.

3.3.1 Sachlicher Anwendungsbereich

Das Recht auf informationelle Selbstbestimmung als Teil des Allgemeinen Persönlichkeitsrechts schützt natürliche Personen (Schild, 2018). Jeder Mensch ist eine natürliche Person. Von der EU-DS-GVO nicht ausdrücklich geschützt sind juristische Personen. Ein Schutz aus dem Allgemeinen Persönlichkeitsrecht könnte nach Art. 19 Abs. 3 GG evtl. auf juristische Personen übertragen werden. Eine pauschale Anwendung scheidet nach Martini (Martini, 2009) jedoch aus, weil das Grundrecht die Persönlichkeitsentfaltung schützt, welche natürlichen Personen vorbehalten ist. Allerdings könnte der Schutz dort wesensgleich auf eine juristische Person angewendet werden, „wo sich die für eine juristische Person agierenden natürlichen Personen in einer grundrechtstypischen Gefährdungslage befinden“ (Martini, 2009). Auch Ziebarth (Ziebarth, 2017, Rn. 13) beschreibt im Rahmen eines Kommentares zur EU-DS-GVO, dass „Daten, die sich auf juristische Personen oder (sonstige) Personenvereinigungen beziehen“, keine personenbezogenen Daten sind. Allerdings kann es Daten geben, die sich zwar „unmittelbar auf eine juristische Person“ beziehen, aber gleichzeitig auch eine natürliche Person betreffen. Ein Beispiel hierfür sind Daten zu einer „Einpersonengesellschaft“.

Wer wird bedroht?			
Staat	Schädigung, Erpressung, Diebstahl von Informationen, IT-Terrorismus	Politische Sabotage, Erreichen eines Informationsvorsprungs	Wirtschaftliche, technische und militärische Spionage, Sabotage, Angriffe auf die IT
	§§ 93ff. StGB, ...		UN-Resolution gegen Spionage
Organisationen	Schädigung, Erpressung, Diebstahl von Informationen, IT-Terrorismus	Wirtschaftliche und technische Spionage, Sabotage	Wirtschaftliche und technische Spionage
	§§ 202a + 202b StGB, ...	Gesetz gegen den unlauteren Wettbewerb, ...	Unternehmerische Freiheit, ...
natürliche Person	Schädigung, Erpressung, Rufmord	Erfassung von Personen und Verhalten, Überwachung von Mitarbeitenden	Staatliche Überwachung, Erfassung und Druckausübung auf politisch Andersdenkende
	Europäische Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, ...		
	natürliche Person	Organisationen	Staat
	Wer bedroht?		

Grafische Darstellung basiert auf (Ström, 2005); Schutznormen wurden ergänzt.

Abbildung 2: Dateninteressent und dadurch in ihren Rechten bedrohte Datenquelle

Verstorbene Personen schützt die EU-DS-GVO ebenfalls nicht – jedoch können diese durch nationales Recht geschützt sein beziehungsweise werden (Ziebarth, 2017, Rn. 11). Dagegen sind ungeborene Embryos (und die sie betreffenden Daten) in jedem Fall geschützt, wobei es unterschiedliche Argumentationen gibt. Teils wird ein eigenständiger Datenschutz angenommen, teils wird er daraus abgeleitet, dass sich die Daten des ungeborenen Kindes immer auch auf die Mutter beziehen (Ziebarth, 2017, Rn. 12).

Aber auch Organisationen und der Staat besitzen Daten, die selbst ohne Bezug zu einer natürlichen Person schützenswert sind. Diese werden zwar nicht durch das Datenschutzrecht beschirmt – es gibt jedoch andere Rechtsgrundlagen für ihren Schutz. Dies ist in Abbildung 2 dargestellt.

Abbildung 2 zeigt auch die unterschiedlichen Akteure. Zwar hat das Datenschutzrecht seine Ursprungsmotivation im Schutz der natürlichen Personen vor dem Staat (Ursache des Volkszählungsurteils von 1983), jedoch entfaltet beispielsweise die EU-DS-GVO auch Schutz gegenüber missbräuchlicher Erhebung, Speicherung und Verarbeitung durch weitere Akteure.

Auch wenn es um die Verarbeitung personenbezogener Daten von natürlichen Personen geht, gibt es im sachlichen Anwendungsbereich Ausnahmen. Ein Beispiel ist die Verarbeitung zu persönlichen und familiären Zwecken: „Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten […] c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ (Artikel 2, Absatz 2, EU-DS-GVO). Auf diese Ausnahme des Anwendungsbereiches können sich jedoch als Verantwortliche nur natürliche Personen berufen, für juristische Personen wie Unternehmen und Vereine gilt diese Ausnahme nicht (Kühling & Raab, 2018, Rn. 23). Damit sich natürliche Personen auf diese Ausnahme berufen können, darf es keinen „Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit“ (Erwägungsgrund 18, EU-DS-GVO) geben. Die EU-DS-GVO gilt sehr wohl für „die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen“ (Erwägungsgrund 18, EU-DS-GVO). Damit ist die Ausnahme eng gefasst. Allerdings umfasst der Begriff „persönliche oder familiäre Tätigkeiten“ nicht nur familiäre Tätigkeiten im Sinne eines formalen Verwandtschaftsverhältnisses, sondern ist im Sinne der anderen Sprachfassungen der EU-DS-GVO haushaltsbezogener zu verstehen (Kühling & Raab, 2018, Rn. 23). Dabei ist noch nicht klar, was alles unter „private und familiäre Tätigkeiten“ zu erfassen ist. Typische

Beispiele dürften „Daten zur eigenen Freizeitgestaltung, zu Hobbys, Urlaub, Unterhaltung, also etwa Adressen und Kontaktdaten (auch elektronisch), Geburtstage [… und andere] Jubiläen“ (Ernst, 2018, Rn. 18) sein.

Die EU-DSG-VO dient also dem Schutz von natürlichen Personen vor den Gefahren durch die Verarbeitung ihrer personenbezogenen Daten. Um den sachlichen Anwendungsbereich zu bestimmen, muss noch geklärt werden, was personenbezogene Daten sind. Die EU-DSG-VO enthält in Artikel 4 Begriffsbestimmungen. Dort werden auch personenbezogene Daten legal definiert:

Definition 3.1:
personenbezogene Daten
*„Im Sinne dieser Verordnung bezeichnet der Ausdruck […] ‚**personenbezogene Daten**‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person”) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;“ (Artikel 4, Nummer 1, EU-DS-GVO)*

„Information“ bezeichnet nach Klabunde (Klabunde, 2017, Rn. 7) „nicht nur Aussagen zu überprüfbaren Eigenschaften oder sachlichen Verhältnissen der betroffenen Person […], sondern auch Einschätzungen und Urteile über sie“. Es kommt dabei ferner nicht auf den Wahrheitsgehalt, die Art der Feststellung (Positiv- beziehungsweise Negativaussagen) oder das Datenformat an (Klabunde, 2017, Rn. 7).

Es wurde bereits erörtert, was eine „natürliche Person“ ist. Jeder Mensch ist eine natürliche Person. Insbesondere der Staat, Gesellschaften wie als Aktiengesellschaft oder GmbH organisierte Unternehmen, als eingetragener Verein organisierte Vereine und Stiftungen sind als juristische Personen keine natürlichen Personen.

Die Bestimmbarkeit (alter Begriff aus dem BDSG bis 2018) beziehungsweise Identifizierbarkeit (Begriff der EU-DS-GVO) kann mit verschiedenen Mitteln erfolgen. Diese zu berücksichtigenden Mittel reichen bei der sogenannten Objektiven Theorie von den der speichernden Stelle zur Verfügung stehenden Mitteln (Bergt, 2015, S. 365f., Ansatz 1) bis hin zur sog. Objektiven Theorie mit allen möglichen Mitteln (Bergt, 2015, S. 366, Ansatz 3). Gemäß der EU-DS-GVO ist es nicht entscheidend, ob der Verantwortliche selbst die Zuordnung zu einer natürlichen Person herstellen kann, es genügt, wenn die Zuordnung für irgendjemand möglich ist. „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“ (Erwägungsgrund 26, EU-DS-GVO). Das allgemeine Ermessen wird weder durch den Erwägungsgrund noch durch die Berücksichtigung von Kosten, zeitlichem Aufwand, verfügbarer Technologie und technologischer Entwicklung konkretisiert. Dadurch ist die Zuordnungsmöglichkeit nicht statisch gegeben oder nicht gegeben, sondern sie kann sich durch technologischen Fortschritt hin zu einer Zuordnungsmöglichkeit verändern (Klabunde, 2017, Rn. 13). Damit ist der Verordnungsgeber einer vermittelnden Theorie gefolgt (Bergt, 2015, S. 366f., Ansatz 4).

Dabei ist es nicht erheblich, ob die Zuordnung zu einer identifizierten beziehungsweise identifizierbaren natürlichen Person mittels einer Kennung (das heißt einem Identifikator) wie

- Namen (beispielsweise Vor- und Nachname)
- Kennnummer (beispielsweise Personalausweisnummer, Sozial-versicherungsnummer, Mitarbeiterstammnummer)
- Standortdaten (beispielsweise Wohnanschrift)
- Online-Kennung (beispielsweise E-Mail-Adresse oder IP-Adresse[6])

[6] Selbst dynamische IP-Adressen sind nach einer Entscheidung des Europäischen Gerichtshofs vom 19.10.2016 personenbezogene Daten, weil die Zuordnung zu einer Person mithilfe des Internetproviders (ggf. mithilfe staatlicher Stellen) möglich ist (EuGH, 19.10.2016 - C-582/14, 2016).

erfolgt oder durch Zuordnung „zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität“ einer Person sind. Im Ergebnis führt sowohl die Kennung/der Identifikator als auch die in einem Kontext einmalige Merkmalkombination zu einer Identifikation.

Die Anwendbarkeit der EU-DS-GVO wird durch Pseudonymisierung nicht beeinträchtigt. In den Erwägungsgründen heißt es dazu: „Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.“ (Erwägungsgrund 26, EU-DS-GVO). Eine Anonymisierung, also eine endgültige Entfernung aller Möglichkeiten zur Identifizierbarkeit und das Vernichten des Originalbestandes (mit Personenbezug) beendet jedoch den Personenbezug und damit die Anwendbarkeit der EU-DS-GVO (Klabunde, 2017, Rn. 16).

3.3.2 Räumlicher Anwendungsbereich

Zunächst gilt das aus der bisherigen europäischen Datenschutzrichtlinie bekannte Niederlassungsprinzip weiterhin. So bestimmt die EU-DS-GVO: „Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.“ (Artikel 3, Absatz 1, EU-DSG-VO)

Der räumliche Anwendungsbereich hat gegenüber der bisherigen Datenschutzrichtlinie allerdings aufgrund des in Artikel 3, Absatz 2 eingeführten Marktortprinzips stark zugenommen: „Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon,

ob von diesen betroffenen Personen eine Zahlung zu leisten ist; b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt." (Artikel 3, Absatz 2, EU-DS-GVO) Demnach kommt es nicht darauf an, wo die Datenverarbeitung erfolgt. Wenn sich ein Angebot an Personen innerhalb der EU richtet oder Personen innerhalb der EU beobachtet werden, ist die EU-DS-GVO selbst dann anwendbar, wenn das Unternehmen keine Niederlassung innerhalb der EU hat. Auch wenn dieses Prinzip keine europäische Besonderheit ist, sondern sich in ähnlicher Form beispielsweise auch im amerikanischen oder auch japanischen Recht findet (Klar, 2018, Rn. 7), ist die globale Durchsetzbarkeit eine Herausforderung. Diese besteht weiterhin. Der Verordnungsgeber versucht beispielsweise durch die Pflicht zur Benennung eines Vertreters innerhalb der EU, die Durchsetzbarkeit der EU-DS-GVO zu verbessern (Klar, 2018, Rn. 27).

3.4 Grundsätze des Datenschutzes der EU-DS-GVO

Die Europäische Datenschutz-Grundverordnung regelt in Artikel 5 neun Grundsätze für die Verarbeitung personenbezogener Daten. Die Grundsätze sind als allgemeine Strukturprinzipien formuliert, Verstöße dagegen werden „besonders scharf" sanktioniert (Pötters, 2018, Rn. 4). Diese sind zunächst in Abbildung 3 dargestellt und werden im Folgenden näher erläutert. Dabei werden Grundsätze, welche durch den modellbasierten Ansatz dieser Arbeit adressiert werden, ausführlicher thematisiert.

3.4.1 Rechtmäßigkeit

Um die Anforderung der Rechtmäßigkeit aus Art. 5, Abs. 1 lit. a, EU-DSG-VO genauer zu analysieren, kann der 40. Erwägungsgrund zur EU-DS-GVO herangezogen werden: „Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden […]" (Erwägungsgrund 40, EU-DSG-VO, Unterstreichung hier vorgenommen). Für eine rechtmäßige Verarbeitung ist also die Einwilligung der be-

troffenen Person oder eine andere Rechtsgrundlage, ein sogenannter Erlaubnistatbestand, erforderlich. In Deutschland wurde dieses Prinzip bisher als „Verbot mit Erlaubnisvorbehalt“ bezeichnet (Pötters, 2018, Rn. 6). Die Erlaubnistatbestände werden in den Artikeln 6 (Rechtmäßigkeit der Verarbeitung) und 9 (Verarbeitung besonderer Kategorien personenbezogener Daten) aufgelistet, zusätzlich sind im nationalen Recht Erlaubnistatbestände möglich, soweit die EU-DSG-VO diese durch eine entsprechende Öffnungsklausel erlaubt (Pötters, 2018, Rn. 6). Durch diese Regelung wird, so Pötters, das häufiger im öffentlichen Recht anzutreffende Prinzip ungewöhnlicherweise auch in das Zivilrecht übertragen und somit faktisch ein Erhebungs- und Verarbeitungsverbot für staatliche und privatwirtschaftliche Akteure mit klar definierten Ausnahmen geschaffen.



Abbildung 3: Grundsätze zur Verarbeitung personenbezogener Daten nach Artikel 5 EU-DSG-VO

Die **Einwilligung** ist im Falle der Verarbeitung personenbezogener Daten durch Unternehmen und sonstige nicht staatliche Akteure der relevanteste Erlaubnistatbestand (Buchner & Kühling, 2017, S. 544). So bezeichnen ihn Wendehorst & Westphalen (Wendehorst & Westphalen, 2016, S. 3745) als den „wichtigste[n] Recht-

fertigungsgrund“. Auch wenn Schulz (Schulz, 2018b, Rn. 4) dieser Bezeichnung widerspricht, ist die Bedeutung für die Praxis aufgrund einer hohen Zahl an Anwendungsfällen gegeben. Einwilligung wird in der EU-DSG-VO definiert:

> *Definition 3.2:*
> *Einwilligung*
> *„Im Sinne dieser Verordnung bezeichnet der Ausdruck: [...] ‚**Einwilligung**‘ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;“ (Artikel 4, Nummer 11, EU-DSG-VO)*

Aufgrund der besonderen Relevanz der Einwilligung auch für die Gestaltung der Geschäftsprozesse (beispielsweise hinsichtlich des Einwilligungszeitpunktes auch als häufiger Erlaubnistatbestand) wird diese hier ausführlicher betrachtet. Die EU-DS-GVO stellt insbesondere folgende Anforderungen an die Einwilligung:

- Vor oder bei Einholung einer Einwilligung muss die betreffende Person **informiert** werden. Dabei müssen insbesondere auch folgende Informationen gegeben werden:
  - Der Betroffene muss über die Zwecke informiert werden, er gibt dann die Einwilligung für „einen oder mehrere bestimmte **Zwecke**“ (Art. 6, Abs. 1, lit. a, EU-DS-GVO). Die Zwecke müssen „so konkret wie möglich benannt werden“ (Schulz, 2018a, Rn. 24).
  - Dazu muss der Betroffene auch wissen, auf welche Daten sich die Einwilligung beziehen soll.
  - Der Betroffene sollte zudem mindestens darüber informiert werden, wer der **Verantwortliche** der Verarbeitung ist (Erwägungsgrund 42, EU-DS-GVO).

- Der Betroffene muss über die Möglichkeit des Widerrufs und die Folgen des Widerrufs der Einwilligung informiert werden (Schulz, 2018b, Rn. 34).

- Der Verantwortliche sollte **nachweisen** können, dass der Betroffene eingewilligt hat (Erwägungsgrund 42, EU-DS-GVO). Gleichwohl ist keine Schriftform vorgeschrieben; so sind beispielsweise auch konkludente Einwilligungen – also Einwilligungen durch schlüssiges Handeln – möglich (Schulz, 2018b, Rn. 42). Allerdings sind weder Stillschweigen noch Opt-out-Verfahren (Kreuz aus einem Kästchen entfernen oder das Setzen eines Kreuzes, um mitzuteilen, dass nicht eingewilligt wird) zulässig (Schulz, 2018b, Rn. 42).
- Die Einwilligung muss **freiwillig** erfolgen (Art. 11, Nr. 11 EU-DS-GVO), es darf kein Druck ausgeübt oder Zwang eingesetzt werden (Schulz, 2018b, Rn. 21). Genauer wird dies im 42. Erwägungsgrund beschrieben: „Es sollte nur dann davon ausgegangen werden, dass sie [*die Person*] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“ (Erwägungsgrund 42, EU-DS-GVO).
    - Die Einwilligung soll für den Fall eines klaren Ungleichgewichtes zwischen dem Verantwortlichen und dem Betroffenen zu keinem gültigen Erlaubnistatbestand führen (Erwägungsgrund 43, EU-DS-GVO). Da der Erwägungsgrund explizit den Fall einer Behörde erwähnt, geht Schulz (Schulz, 2018b, Rn. 23) davon aus, dass der Verordnungsgeber rechtliche Abhängigkeitsverhältnisse regeln wollte. Diese könnten beispielsweise noch in Arbeitsverhältnissen oder bei akuten Behandlungen durch Krankenhäuser/Ärzte vorliegen[7].

[7] Nach Schulz (Schulz, 2018b, Rn. 23) sollte dies besser durch einen anderen – gesetzlichen – Erlaubnistatbestand geregelt werden.

    - Die Bedingung der Freiwilligkeit wird auch durch das **Kopplungsverbot** in Art. 7 Abs. 4 EU-DS-GVO weiter gestärkt. Die Formulierung „im größtmöglichen Umfang“ (Art. 7, Abs. 4, EU-DS-GVO) lässt erkennen, dass das Kopplungsverbot nicht absolut ist (Schulz, 2018b, Rn. 26)[8]. Im Allgemeinen darf aber bei einem Dienstleistungsvertrag keine Einwilligung abverlangt werden, die zur Erbringung der Dienstleistung nicht erforderlich ist (Ernst, 2017, S. 112). Zum Kopplungsverbot gehört nach Erwägungsgrund 43 das Verbot, zu verschiedenen Verarbeitungsvorgängen nur zusammen eine Einwilligung zu verlangen, obwohl die Trennung angebracht wäre (Schulz, 2018b, Rn. 25). Damit soll der Betroffene in eine Verarbeitung einwilligen, die andere Einwilligung aber versagen können.

- Die Einwilligung muss von der betroffenen Person **höchstpersönlich** erklärt werden (Ernst, 2017, S. 111). Es ist nicht möglich, eine Einwilligung für Dritte abzugeben. So ist es beispielsweise auch nicht möglich, für einen Adressbuchkontakt gegenüber einem Messenger die Einwilligung zu erteilen (Schulz, 2018b, Rn. 8). Bezüglich der Einwilligung von Minderjährigen (hier relevant sind Minderjährige unter 16 Jahren) enthält Art. 8 EU-DS-GVO zwei Möglichkeiten: Entweder die Eltern (Erziehungsberechtigten) willigen für den Minderjährigen ein oder der Minderjährige willigt selbst

[8] Ein Beispiel, das die Schranken des Kopplungsverbots verdeutlicht, ist die Beachtung der Interessen und insbesondere des Geschäftsmodells des Verantwortlichen. So soll es weiter möglich sein, einen Dienst zu erbringen, der „nur […] durch die – einwilligungsbasierte – Verarbeitung der Nutzerdaten (auch) zu Werbezwecken Dritter“ (Schulz, 2018b, Rn. 27) finanzierbar ist. Die Erbringung solcher Dienste soll auch weiterhin (ohne Bezahlschranken) möglich sein (so auch Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 2017). Das Beispiel von verschiedenen Zeitungswebseiten zeigt aktuell aber bereits die Möglichkeit, dem Nutzer die Wahl zu geben, entweder eine entsprechende Einwilligung zu erteilen oder für den Inhalt zu bezahlen.
Schulz (Schulz, 2018b, Rn. 31) nimmt für einige Fälle (beispielsweise kostenloses E-Mail-Konto mit Gegenfinanzierung durch individualisierte Werbung) hier keine einwilligungsbasierte Datenverarbeitung an, sondern geht davon aus, dass es sich um ein „synallagmatisches vertragliches Austauschverhältnis ([… Dienst] gegen die Möglichkeit der Datennutzung)“ (Schulz, 2018b, Rn. 30) handelt. Dann kann mit Erwägungsgrund 44 gelten: „Die Verarbeitung von Daten sollte als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist“ (Erwägungsgrund 44, EU-DS-GVO). Das hat auch den Vorteil, dass die betroffene Person die Einwilligung nicht widerrufen (und weiter die Leistungen beziehen) kann, sondern den Vertrag insgesamt kündigen muss.

ein und die Eltern geben vorher dazu ihre Einwilligung oder willigen nachträglich in Form einer Zustimmung ein (Schulz, 2018c, Rn. 17).

- Die EU-DSG-VO unterscheidet besondere Kategorien personenbezogener Daten von normalen personenbezogenen Daten. Im Rahmen von Geschäftsprozessen müssen die Kategorien auch unterschieden werden, weil unterschiedliche Verarbeitungsbedingungen gelten. Die besonderen Kategorien sind wie folgt definiert:

Definition 3.3:
besondere Kategorien personenbezogener Daten
„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.“ (Art. 9, Abs. 1, EU-DSG-VO)

Auch dieses Verbot wurde als Verbot mit Erlaubnisvorbehalt ausgestaltet. So heißt es: „[Artikel 9] Absatz 1 gilt nicht in folgenden Fällen: a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach [Artikel 9] Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden […]“ (Art. 9, Abs. 2, EU-DS-GVO). Einen Erlaubnistatbestand bildet also wieder die Einwilligung. An sie sind jedoch zusätzlich besondere Bedingungen geknüpft. Dazu gehören:

- Unionsrecht oder nationales Recht können für bestimmte Fälle vorsehen, dass eine Einwilligung das Verbot nicht aufgeben kann. Dadurch ist es möglich, den Datenschutz – auch in einzelnen Mitgliedsstaaten – für diese besonderen Kategorien weiter zu schärfen (Schulz, 2018d, Rn. 19).

- Die Einwilligung muss „ausdrücklich“ sein. Der Verordnungsgeber wollte damit eine besonders hohe Hürde schaffen, wie genau diese ausgestaltet sein soll, ist jedoch unklar (Schulz, 2018d, Rn. 16).

Die Weiterverarbeitung von Daten ist bei Zweckerreichung beziehungsweise Wegfall des Zweckes und bei Widerruf unzulässig (Schulz, 2018a, Rn. 26). Geschäftsprozesse sind also so zu gestalten, dass bei Zweckerreichung oder Wegfall des Zweckes keine weitere Verarbeitung erfolgt. Da der Zweck regelmäßig durch einen Geschäftsprozess erreicht wird, kann die Einwilligung gleichzeitig als nicht mehr wirksam (weil Zweck erreicht) markiert werden. Beim Wegfall der Zwecke etwa durch ein verändertes Geschäftsmodell ist dies schwieriger zu implementieren und wird insbesondere für laufende Geschäftsprozessinstanzen oft manuell durchgesetzt werden müssen.

Der Widerruf muss dabei einfach und jederzeit möglich sein, der Verantwortliche darf jedoch den Betroffenen auf implementierte Widerspruchsmöglichkeiten über übliche Kommunikationsmittel verweisen (Schulz, 2018b, Rn. 56). Dies ist für die Gestaltung von Geschäftsprozessen (konkret eines Prozesses zur Verarbeitung von Widerrufen) vorteilhaft. Der Widerruf gilt nicht rückwirkend, die bisherige Verarbeitung kann sich also weiter auf die Einwilligung berufen, aber eine Weiterverarbeitung kann sich nicht mehr auf die Einwilligung stützen – sog. Ex-nunc-Wirkung (Schulz, 2018b, Rn. 54). Geschäftsprozesse müssen also, wenn sie sich auf den Erlaubnistatbestand Einwilligung beziehen, bei jeder Verarbeitung von personenbezogenen Daten (und insbesondere in länger laufenden Geschäftsprozessinstanzen auch bei jedem Verarbeitungsschritt) prüfen, ob eine nicht widerrufene Einwilligung vorliegt. Davon unabhängig können sich an einen ausgeübten Widerruf der Einwilligung durch den Betroffenen weitere Schritte anschließen, dazu gehört beispielsweise die Löschung der Daten nach Art. 17 EU-DSG-VO (Schulz, 2018b, Rn. 56).

Außer der Einwilligung kommen weitere Erlaubnistatbestände in Betracht. Für unternehmerische Prozesse relevant wird auch der **Erlaubnistatbestand der für die Vertragserfüllung notwendigen Datenverarbeitung** (Art. 6, Abs. 1, lit. b, EU-DS-GVO) sein. Dabei muss eine Vertragspartei die betroffene Person sein. Explizit auch

erlaubt wird die Verarbeitung als **vorvertragliche Maßnahme**, sofern eine entsprechende Anfrage der betroffenen Person zugrunde liegt. Dieser Erlaubnistatbestand kommt auch als „synallagmatisches vertragliches Austauschverhältnis ([… Dienst] gegen die Möglichkeit der Datennutzung)“ (Schulz, 2018b, Rn. 30) auch bei kostenlosen Diensten in Betracht (vergleiche Fußnote 8). Wie der Erlaubnistatbestand der Einwilligung geht auch die Verarbeitung zur Erfüllung eines Vertrages beziehungsweise als vorvertragliche Maßnahmen auf den Willen des Betroffenen (hier zum Vertragsschluss oder zur Vertragsanbahnung) zurück (Schulz, 2018a, Rn. 27+28). Dabei muss die Verarbeitung für die Erfüllung von Pflichten des Vertrages (konkret seiner Haupt- und Nebenpflichten) oder zur Wahrnehmung von Vertragsrechten erforderlich sein und die betroffene Person muss selbst Partei des Vertrages sein (Schulz, 2018a, Rn. 38). Konkret ist die „Erforderlichkeit […] nicht gegeben, wenn die Interessen auch ohne die Kenntnis der personenbezogenen Informationen gewahrt werden können“ (Schulz, 2018a, Rn. 38). Die Erforderlichkeit ist von der reinen Zweckdienlichkeit abzugrenzen, so reicht es nach Buchner & Petri (Buchner & Petri, 2018, Rn. 42) nicht aus, dass eine Verarbeitung „irgendwie ‚dienlich‘ oder ‚nützlich‘“ ist, und auch das Ziel einer beschleunigten Abwicklung genügt hierzu nicht.

Andere Erlaubnistatbestände, welche eine Ausnahme vom Verbot der Verarbeitung personenbezogener Daten bilden, sind gemäß Artikel 6, Absatz 1 EU-DS-GVO:

- Rechtliche Verpflichtung (Art. 6, Abs. 1, lit. c, EU-DS-GVO): Wenn der Verantwortliche die Daten aufgrund einer rechtlichen Verpflichtung verarbeiten muss, darf er dies im notwendigem Umfang auch. Eine rechtliche Verpflichtung kann sich beispielsweise aus den Buchführungs- und Nachweispflichten des Handelsgesetzbuches beziehungsweise der Abgabenordnung (nationales Recht) ergeben (Schulz, 2018a, Rn. 44).
- Schutz von „lebenswichtige[n] Interessen der betroffenen Person oder einer anderen natürlichen Person“ (Art. 6, Abs. 1, lit. d, EU-DS-GVO). Wenn eine Verarbeitung notwendig ist, um lebenswichtige Interessen einer natürlichen Person zu schützen, ist sie zulässig. Dabei spielt es keine Rolle, ob es

sich um die Interessen der betroffenen Person oder einer dritten natürlichen Person handelt. Es geht hier beispielsweise um die Abwendung einer Gefahr für das Leben oder die körperliche Unversehrtheit (Erwägungsgrund 112, EU-DS-GVO). Dabei kann die Datenverarbeitung möglichen Opfern von Straftaten „Leib, Leben und Freiheit (auch: Entführung, Herbeiführung einer Sprengstoffexplosion) oder der Abwehr schwerer Gefährdungslagen" (Frenzel, 2018, Rn. 20) dienen.

- Erfüllung öffentlicher Aufgaben (Art. 6, Abs. 1, lit. e, EU-DS-GVO). Nach Frenzel (Frenzel, 2018, Rn. 23) ist dieser Erlaubnistatbestand neben der Einwilligung der wichtigste Erlaubnistatbestand. Es kommt dabei nicht auf den Verantwortlichen an (dieser kann beispielsweise auch hier eine Behörde, ein Unternehmen, aber auch eine Privatperson sein), sondern es geht um die öffentliche Aufgabe an sich. Damit eine Verarbeitung durch den Verantwortlichen zulässig ist, muss ihm die Aufgabe aber übertragen worden sein (Frenzel, 2018, Rn. 25). Ein Beispiel ist die staatliche Verkehrsüberwachung durch Videosysteme (Buchner & Petri, 2018, Rn. 138).
- Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6, Abs. 1, lit. f, EU-DS GVO). Dieser Erlaubnistatbestand wird aber bereits im Wortlaut wieder eingeschränkt. Die Verarbeitung muss nicht nur erforderlich sein, es dürfen auch „nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen" (Art. 6, Abs. 1, lit. f, EU-DS GVO). Zudem werden Kinder in der Interessensabwägung nochmals besonders geschützt. Gemäß Art. 6, Abs. 1, S. 2 können sich jedoch Behörden in Erfüllung ihrer Aufgaben nicht auf diesen Erlaubnistatbestand berufen. Die Bestimmung wird in Erwägungsgrund 47 der EU-DS-GVO näher erläutert. Dennoch verbleibt bei Berufung auf diesen Erlaubnistatbestand eine große Rechtsunsicherheit, die sich aus den vagen Formulierungen ergibt (Schulz, 2018a, Rn. 60+61). Ein möglicher Anwendungsfall ist die IT-Sicherheit von elektronischen Kommunikationsnetzen (Buchner & Petri, 2018, Rn. 167),

ein anderer der Betrieb von Suchmaschinen oder eines Dienstes zur Warnung vor möglichem Versicherungsbetrug (Buchner & Petri, 2018, Rn. 171+173-174).

3.4.2 Verarbeitung nach Treu und Glauben

Der Grundsatz Treu und Glauben ist in Art. 5, Abs. 1, lit. a, EU-DS-GVO bestimmt. Der Begriff „Treu und Glauben" darf nicht mit dem gleichen Begriff in § 242 BGB gleichgesetzt werden, sondern muss unbedingt autonom im Kontext des Unionsrechts ausgelegt werden. Er ist allerdings gleichzeitig schwer positiv zu erläutern (Pötters, 2018, Rn. 8). Leichter ist das ungewollte treuwidrige Verhalten zu beschreiben, um so ein Verständnis des Begriffes zu erhalten. Treuwidrig ist u. a. der Einsatz verborgener Techniken (diese verstoßen auch gegen den Grundsatz der Transparenz) wie Spyware oder heimliche Videoüberwachung, die Verletzung des Zweckbindungsgrundsatzes und der Einsatz unangemessener, unverhältnismäßiger oder nicht erforderlicher Mittel (Pötters, 2018, Rn. 9). Dazu erscheint ein Verweis auf einen Verstoß gegen das Prinzip Treu und Glauben aber nicht notwendig, da die Verarbeitung schon durch konkretere Vorschriften rechtswidrig ist. Dafür spricht auch die Sichtweise von Reimer: Das Prinzip Treu und Glauben „stellt eine Generalklausel bereit, nach der gewisse Verarbeitungen als verboten behandelt werden können […], selbst wenn sie mit allen datenschutzrechtlichen Einzelregelungen im Einklang stehen" (Reimer, 2017, Rn. 14). Eine andere mögliche Bezeichnung wäre analog zum englischsprachigen Wortlaut „fairly" der Begriff „Fairness" beziehungsweise konkrete „Gewährleistung einer ‚fairen' Verarbeitung" gewesen (Heberlein, 2017, Rn. 9).

3.4.3 Transparenz

Ebenfalls in Art. 5, Abs. 1, lit. a, EU-DS-GVO wird der Grundsatz der Transparenz geregelt. Er setzt voraus, dass der Betroffene alle Informationen und Mitteilungen über die Verarbeitung seiner personenbezogenen Daten leicht auffinden kann, sie sollen aber zusätzlich auch verständlich sowie in klarer und einfacher Sprache verfasst sein

(Erwägungsgrund 39, EU-DS-GVO). Die Information des Betroffenen dazu ist ebenfalls wichtig, damit der Betroffene seine Rechte beispielsweise bezüglich Auskunft, Berichtigung und Löschung geltend machen kann (Pötters, 2018, Rn. 11).

3.4.4 Zweckbindung

Die Zweckbindung ist in Art. 5, Abs. 1, lit. b, EU-DS-GVO festgeschrieben. Im Wortlaut wird bestimmt: „Personenbezogene Daten müssen […] für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; […] (‚Zweckbindung')“ (Art. 5, Abs. 1, S. 1 und lit. b, EU-DS-GVO). Da auch die Zweckbindung für die Geschäftsprozesse von Unternehmen entscheidend sein kann, soll auch diese hier etwas ausführlicher betrachtet werden.

Die Zwecke müssen also festgelegt sein, das heißt, sie müssen bereits vor Erhebung der Daten feststehen (Pötters, 2018, Rn. 16). Auch sollten sie schriftlich festgehalten sein, eine reine gedankliche Festlegung genügt nicht (Reimer, 2017, Rn. 20). Diese Forderungen sind unabhängig vom Erlaubnistatbestand. Beim Erlaubnistatbestand der Einwilligung wird nur zusätzlich gefordert, dass der Betroffene in genau diese Zwecke vorher eingewilligt hat. Dies ist jedoch dann schwierig, wenn Verarbeitungen zu unspezifischen Zwecken erfolgen sollen, wie es beispielsweise im Falle von Big-Data-Analysen aufgrund der Ergebnisoffenheit regelmäßig der Fall ist. Dieser Anwendungsfall ist von der EU-DS-GVO nicht hinreichend geregelt (Schulz, 2018a, Rn. 255)[9].

Die Zweckangabe muss zudem eindeutig sein, sie darf insbesondere nicht zu breit sein oder unklar umschrieben werden (Pötters, 2018, Rn. 14). Die Zwecke müssen zudem legitim, das heißt rechtlich zulässig sein.

[9] Die Lösung für Einwilligungen in eine ergebnisoffene Big-Data-Verarbeitung könnten entweder eine Generaleinwilligung oder sog. gestufte Einwilligungen sein (Schulz, 2018b, Rn. 35). Diese sind bereits aus der medizinischen Forschung bekannt. Der Betroffene kann dann entweder vorab entscheiden, welche denkbaren Zwecke er zulassen beziehungsweise verbieten möchte oder in der jeweiligen Phase zunächst in die Analyse selbst und später in die Nutzung der Analyseergebnisse für bestimmte Zwecke einwilligen (Schulz, 2018b, Rn. 35).

Auch eine Weiterverarbeitung wird durch die Zwecke der Erhebung eingeschränkt.

Eine Weiterverarbeitung ist konkret neben dem ursprünglichen Zweck nur in einer mit dem ursprünglichen Zweck zu vereinbarenden Weise zulässig. Dabei kommt es nach Reimer (Reimer, 2017, Rn. 24) gemäß dem Wortlaut auf die Weise und nicht auf den Zweck der Weiterverarbeitung an.

Nach Herbst (Herbst, 2018, Rn. 42) meint der Begriff „Weiterverarbeitung" der EU-DS-GVO eine Zweckänderung. Die Weiterverarbeitung für den neuen Zweck beziehungsweise die Zweckänderung sei nur zulässig, wenn die zwei folgenden Voraussetzungen beide erfüllt sind:

- „Eine solche Weiterverarbeitung zu geänderten Zwecken ist nur zulässig, wenn kumulativ zwei Voraussetzungen erfüllt sind: Die Weiterverarbeitung zu dem neuen Zweck darf nicht mit dem bei der Datenerhebung festgelegten Zweck unvereinbar sein (Erfordernis der Zweckvereinbarkeit)." (Herbst, 2018, Rn. 42)
- „für die Weiterverarbeitung zu dem neuen Zweck muss eine ausreichende Rechtsgrundlage vorhanden sein" (Herbst, 2018, Rn. 42).

Ob die zweite Voraussetzung erfüllt sein muss, ist allerdings nach Herbst umstritten. Heberlein (Heberlein, 2017, Rn. 19) vertritt ebenfalls die Ansicht, dass beide Voraussetzungen erfüllt sein müssen. Zudem bestimmt die EU-DS-GVO, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke" (Art. 5, Abs. 1, lit. b, EU-DS-GVO) nicht als mit dem ursprünglichen Zweck unvereinbar gilt.

3.4.5 Datenminimierung

Verarbeitete personenbezogene Daten müssen „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung")" (Art. 5, Abs. 1, lit. c, EU-DS-GVO).

Die Zwecke der Datenverarbeitung gemäß der Zweckbindung sind also relevant, um die Menge der verarbeiteten Daten zu bestimmen. Die Menge soll unter dem Stichwort Datenminimierung beschränkt sein. Dabei gelten drei Kriterien:

- Die Daten müssen für den Zweck angemessen sein. Das heißt, die verarbeiteten Daten müssen einen Bezug zum Zweck haben (Herbst, 2018, Rn. 57). Nach Frenzel (Frenzel, 2018, Rn. 35) darf dieser nicht zu beanstanden sein (das heißt, der Bezug muss legitim sein).
- Die Daten müssen für den Zweck erheblich sein. Das heißt, sie müssen geeignet sein, um den Zweck zu erreichen (Herbst, 2018, Rn. 57).
- Die Daten müssen für den Zweck der Verarbeitung notwendig sein. Eine Kontrollfrage dazu kann lauten: Ist es möglich, den Verarbeitungszweck ohne die Daten (evtl. mit weniger Daten) zu erreichen?
  Nach Herbst (Herbst, 2018, Rn. 57+58) ist auch zu bedenken, ob der Zweck nicht auch mit aggregierten oder anonymisierten Daten erreicht werden kann. Auch eine Pseudonymisierung kommt als Maßnahme der Datenminimierung infrage (Pötters, 2018, Rn. 23).

Dabei ist nicht nur die „Anzahl der verarbeiteten Daten", sondern auch die „Anzahl der Nutzungen" und die „Anzahl der Betroffenen" einzuschränken (Pötters, 2018, Rn. 22). Es würden auch technische Maßnahmen dazugehören wie beispielsweise die reine Anzeige der Daten auf einem Bildschirm ohne Möglichkeit der Vervielfältigung beziehungsweise des Ausdrucks (Pötters, 2018, Rn. 22+23).

3.4.6 Richtigkeit

Nach Art. 5, Abs. 1, lit. d, EU-DS-GVO muss der Verantwortliche dafür Sorge tragen, dass die Daten sachlich richtig und, sofern erforderlich, auch auf dem neuesten Stand sind. Der Verantwortliche muss dazu die erforderlichen Maßnahmen treffen. Damit hat der Verantwortliche unabhängig vom Berichtigungsanspruch des Betroffenen ebenfalls für die Richtigkeit der Daten zu sorgen (Pötters, 2018, Rn. 24).

3.4.7 Speicherbegrenzung

Die Speicherbegrenzung bestimmt, dass personenbezogene Daten „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“ (Art. 5, Abs. 1, lit. e, EU-DS-GVO). Der Verantwortliche muss nach (Pötters, 2018, Rn. 25) Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen; diese Bestimmung konkretisiert die Zweckbindung in zeitlicher Hinsicht. Alternativ zur Löschung kann der Personenbezug entfernt werden (Herbst, 2018, Rn. 66). Analog zur Datenminimierung wird hier der Verantwortliche unabhängig von den Betroffenenrechten (Recht auf Löschung gemäß Art. 17, Abs. 1 lit. a, und Recht auf Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 EU-DS-GVO) verpflichtet, die Speicherung (mindestens hinsichtlich des Personenbezugs) zu begrenzen. Er muss zudem den Betroffenen über die Speicherdauer informieren beziehungsweise, falls diese nicht feststeht, über die Kriterien, nach denen die Dauer festgelegt wird (Pötters, 2018, Rn. 26).

3.4.8 Vertraulichkeit und Integrität

Artikel 5, Abs. 1 lit. f, EU-DS-GVO fordert die Gewährleistung einer angemessenen Sicherheit im Allgemeinen und von Vertraulichkeit und Integrität im Speziellen durch geeignete technische und organisatorische Maßnahmen. Es geht hier nicht um einen

zusätzlichen materiell-rechtlichen Schutz[10], sondern um spezifische Vorgaben hinsichtlich der Informationssicherheit der verarbeitenden Systeme beziehungsweise der Daten (Pötters, 2018, Rn. 28). Dabei ist sowohl vor unbefugter als auch vor unrechtmäßiger Verarbeitung zu schützen. Gleichzeitig umfassen die unbefugten Verarbeitungen alle Verarbeitungen, die „gegen den Willen des Verantwortlichen" stattfinden (Reimer, 2017, Rn. 49). Unrechtmäßige Verarbeitungen umfassen solche, die gegen die Bestimmungen des Datenschutzrechtes verstoßen (andere Gesetze seien hier nicht relevant, diese seien durch unbefugt abgedeckt), also beispielsweise sich auf keinen Erlaubnistatbestand berufen können (auch ein Hacker bräuchte für eine datenschutzrechtmäßige Verarbeitung einen solchen Erlaubnistatbestand) (Reimer, 2017, Rn. 48).

3.4.9 Rechenschaftspflicht

Nachdem Artikel 5 Absatz 1 EU-DS-GVO die vorgenannten acht Grundsätze festgelegt hat, wird der Verantwortliche vom 2. Absatz dazu verpflichtet, die Grundsätze einzuhalten und diese Einhaltung auch nachweisen zu können. Diese Rechenschaftspflicht ist sowohl gegenüber der bisherigen europäischen Datenschutzrichtlinie als auch gegenüber dem nationalen Bundesdatenschutzgesetz eine „echte Veränderung" und damit in dieser Intensität eine neue Anforderung für die Verantwortlichen (Jung, 2018, S. 208f.). Das „Nachweisen-Können-Müssen" wird auch in Artikel 24 Absatz 1 EU-DS-GVO konkretisiert (Veil, 2018, S. 9). Verantwortliche (also beispielsweise Unternehmen) müssen daher nun erstmals einen „systematischen Nachweis ordnungsgemäßer Datenverarbeitung" (Jung, 2018, S. 208) hinsichtlich des Datenschutzes sicherstellen. Jung (Jung, 2018) empfiehlt daher den Aufbau eines „Datenschutz-(Compliance-)Management-System[s]". Dabei ist zwischen prozessunabhängiger, das heißt nicht an eine spezifische Datenverarbeitung gebundene Dokumentation (wie beispielsweise der Nachweis von Datenschutzschulungen oder die Bestellung eines

[10] Ein zusätzliches materielles Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat dagegen das Bundesverfassungsgericht in einem Urteil vom 27. Februar 2008 geschaffen (BVerfG, 2008).

Datenschutzbeauftragten) und prozessabhängiger Dokumentation zu unterscheiden (Jung, 2018, S. 212).

Eine systematische Modellierung aller Prozesse mit Verarbeitung von personenbezogenen Daten, beispielsweise mit den Ansätzen der vorliegenden Arbeit, kann einen wichtigen Beitrag zur Erfüllung dieser Rechenschaftspflichten leisten.

4 Grundlagen: Unternehmensmodellierung

4.1 Modellierung

In diesem Abschnitt werden einführend die Grundlagen zu Modellen und Modellierung betrachtet. Da Modelle in verschiedensten Disziplinen verwendet werden, gibt es eine große „Diversität von Modellen“ (Thalheim & Nissen, 2015, S. 491) und kein einheitliches Verständnis des Modellbegriffs und der Modellierung. Auch wenn es, um die Zusammenarbeit zwischen Forschergruppen zu fördern, Bemühungen um einen interoperablen und übergreifenden Modellbegriff gibt, ist die Arbeit daran noch nicht abgeschlossen. Für die in dieser Arbeit untersuchten Fragestellungen sind verschiedene Wissenschaftsdisziplinen – insbesondere die Wirtschaftswissenschaften, die Informatik und die Rechtswissenschaften – von Bedeutung. Diese Wissenschaftsdisziplinen haben jedoch untereinander und teils auch innerhalb der Wissenschaftsdisziplinen kein einheitliches Verständnis des Modellbegriffs. Für die Disziplinen Informatik, Wirtschaftsinformatik und Betriebswirtschaftslehre stellt dies beispielsweise Thomas (Thomas, 2005, S. 7) fest. Für die Rechtswissenschaften analysiert Schuhr (Schuhr, 2006, S. 224f.) die Verwendung des Begriffs Modell. Ein Verwendungsbeispiel ist das „Europäische Modellstrafgesetzbuch“, das Vorbild für nationale Gesetzgebung („Kodifikation“) ist. Ein anderes Beispiel sind die „verschiedenen Modelle der Vertragsgestaltung“, wie beispielsweise „Timesharing-Modelle“ und „Finanzierungsmodelle“. Sie zeigen eine Verwendung des Begriffs Modelle als „rechtliche Konstruktionen“. Die beiden ausgewählten Beispiele zeigen bereits, dass das Verständnis des Begriffs Modells in den Rechtswissenschaften mindestens teilweise von dem in der Informatik oder den Wirtschaftswissenschaften abweicht.

Um nachfolgend ein einheitliches Begriffsverständnis zu haben, werden zunächst in Definition 4.1 die Begriffe Modell, Modelloriginal, Sicht und Modellierung definiert (Stachowiak, 1973, S. 128 ff.).

Definition 4.1:
Modell, Modelloriginal, Sicht und Modellierung

- *Ein **Modell** ist ein vereinfachtes Abbild eines Modelloriginals.*
- *Jedes Modell dient einem bestimmten Zweck. Zusätzlich ist es eventuell nur für bestimmte Modellnutzer (Zielgruppen), Untersuchungen, Überlegungen, Operationen und für einen bestimmten Zeitraum bestimmt. Die Vereinfachung bei der Abbildung ist entsprechend dem Zweck zu wählen.*
- *Ein **Modelloriginal** kann entweder a) die Realität, b) ein erdachtes (evtl. rein gedankliches) System oder c) ein Ausschnitt von a) oder b) sein.*
- *Zu einem Modelloriginal können für verschiedene Zwecke verschiedene Aspekte eines Modelloriginals in verschiedenen Modellen abgebildet werden. Man spricht von verschiedenen **Sicht**en beziehungsweise Perspektiven auf ein Modelloriginal.*
- ***Modellierung** bezeichnet den Vorgang der Erstellung eines Modells.*

Modellierung wird nach Holten (Holten, 2000) als „Vorgang verstanden, bei dem ein Modellierer, der einen Sachverhalt in der realen oder gedachten Welt wahrnimmt, auf Basis dieser Wahrnehmung ein Abbild dieses Sachverhaltes konstruiert". Allerdings werden Modelle nicht immer von natürlichen Personen als Modellierer konstruiert, sondern teils auch automatisch erzeugt. Als Beispiele seien ein 3-D-Scanner bei der Erfassung der Oberfläche eines Objektes (Modelloriginal) oder Software zur Erzeugung eines Klassenmodells zu einer als Quellcode vorliegenden anderen Software genannt.

Die Modellierung orientiert sich an den drei Hauptmerkmalen des allgemeinen Modellbegriffs nach Stachowiak (Stachowiak, 1973, S. 131ff.):

- Abbildungsmerkmal: Modelle sind Abbildungen beziehungsweise Repräsentationen eines Modelloriginals. Dabei kann das Modelloriginal nach Stachowiak (Stachowiak, 1973) natürlich oder künstlich sein, sogar Modelle könnten selbst wieder als ein Modelloriginal für ein anderes Modell dienen. Die Abbildung muss nach Thalheim & Nissen (Thalheim & Nissen, 2015, S. 496) so erfolgen, dass das Modell das Original adäquat und verlässlich repräsentiert.
- Verkürzungsmerkmal, das heißt Vereinfachung: Modelle erfassen nicht das gesamte Modelloriginal. Bei der Modellierung wird ein Ausschnitt des Originals ausgewählt und festgelegt, welche Attribute des Modelloriginals abgebildet werden sollen. Attribut bezeichnet hier entweder eine Eigenschaft oder eine Beziehung oder eine Operation eines Modelloriginals. Auch abgebildete Attribute, wie beispielsweise Beziehungen, können ihrerseits Attribute haben. Wichtig ist, dass die Vereinfachung „in einer Weise" vorgenommen wird, die von der Zielgruppe akzeptiert wird (Kaschek, 1999).
- Pragmatisches Merkmal: Modelle erfüllen ihre Ersetzungsfunktion nur für bestimmte Zwecke. Das bedeutet auch, dass ein Modell für bestimmte „gedankliche oder tatsächliche Operationen" (Stachowiak, 1973, S. 133) konzipiert und dementsprechend darauf beschränkt sein kann. Auch kann sich ein Modell an bestimmte Modellnutzer richten, Modellnutzer können Menschen, aber auch IT-Systeme[1] sein.

  Die Zweckbindung ermöglicht es, eine zweckgemäße Vereinfachung vorzunehmen. Nach Jeanneret u. a. (Jeanneret, Glinz & Baar, 2012) bildet ein klar spezifizierter Zweck einen Vertrag zwischen Modellierer und Modellnutzer. Der Modellnutzer kann dementsprechend Zweck, aber auch Grenzen des Modells erkennen. Nach Schuhr (Schuhr, 2006, S. 223) ist es wichtig, dass

[1] Bereits Stachowiak (Stachowiak, 1973) spricht neben Menschen von einem möglichen „künstlichen Modellbenutzer".

der Modellnutzer sich über Abstraktionen und Idealisierung des Modells bewusst ist.

Vereinfachung und Abbildung werden beide zusammen auch als Transformation bezeichnet. Vereinfachung und Abbildung haben beide zur Folge, dass die Wahrnehmung des Modellierers hinsichtlich des Modelloriginals, aber auch hinsichtlich der Bedürfnisse der Modellnutzer das Modell mitprägt. Auch die Interpretation eines Modells ist nicht immer eindeutig, die Wahrnehmung des Modellnutzers kann von Bedeutung sein. Diese sogenannten Transformationseffekte (K. Pohl, 2008) können nicht völlig vermieden, aber durch eine geeignete Vorgehensweise deutlich reduziert werden. Ein Beispiel für einen solchen Effekt ist die Abundanz. Das bedeutet, dass ein Modellattribut im Modell vorhanden ist, das keine Entsprechung im Original hat (Stachowiak, 1973). Diese Modellattribute können durch implizite oder explizite Annahmen des Modellierers entstehen. Modellattribute ohne Entsprechung im Modelloriginal dürfen nicht ausgewertet werden, da sonst fehlerhafte Schlüsse entstehen können.

Modelle können dazu dienen, die Sprachfähigkeit über ein Modelloriginal zu erhöhen, das Modelloriginal zu analysieren oder ein zukünftiges System zu planen. Modelle können auch das Ziel haben, ein System zu bauen[2] beziehungsweise zu steuern.

Modelle lassen sich insbesondere mithilfe von natürlicher Sprache, Grafik, mathematischer Struktur und/oder dreidimensionalen Plastiken darstellen. In vielen Fällen wird für die Darstellung eine Modellierungssprache verwendet. Modellierungssprachen ermöglichen und beschränken die Nutzbarkeit von Modellen (Thalheim & Nissen, 2015, S. 500). Modellierungssprachen definieren gemäß Karagiannis & Kühn (Karagiannis & Kühn, 2002) einerseits die Syntax eines Modells, das heißt, sie legen die gültigen Modellelementtypen sowie die gültigen Kombinationen fest. Anderer-

[2] Im Bereich der Softwareentwicklung wird dies als Modellgetriebene Softwareentwicklung (MDSD, englisch: model-driven software development) bezeichnet.

seits geben Modellierungssprachen die Semantik der verschiedenen Modellelementtypen sowie deren Kombinationen vor. Damit legen sie den Grundstein für die spätere Interpretation.

Die Benutzerfreundlichkeit einer Modellierungssprache muss anhand verschiedener Kriterien bewertet werden. Schalles u. a. haben dazu die Kriterien „Erlernbarkeit, Einprägsamkeit, Effektivität, Effizienz, Benutzerzufriedenheit sowie visuelle Wahrnehmung“ (Schalles, Rebstock & Creagh, 2010, S. 18f.) aus der allgemeinen Usability-Literatur herausgearbeitet und auf Modellierungssprachen übertragen.

Abbildung 4 veranschaulicht den Zusammenhang zwischen Modelloriginal, Modellen und Sichten. Zu einem Modelloriginal können verschiedene Modelle existieren. Dabei können auch mehrere Modelle zur gleichen Sicht gehören (In der Abbildung gehören das Modell 2 und das Modell 3 zur Sicht II.) und den gleichen Aspekt mit einer anderen Darstellung beschreiben. Die Modelle entstehen durch eine Abbildungsfunktion. Dadurch wird das Modelloriginal vereinfacht, das heißt verkürzt, dargestellt. Außerdem kann eine Sicht auf ein Modelloriginal verschiedene Aspekte und verschiedene bereits existierende Sichten umfassen. In der Abbildung wird dies als integrierte Sicht bezeichnet.

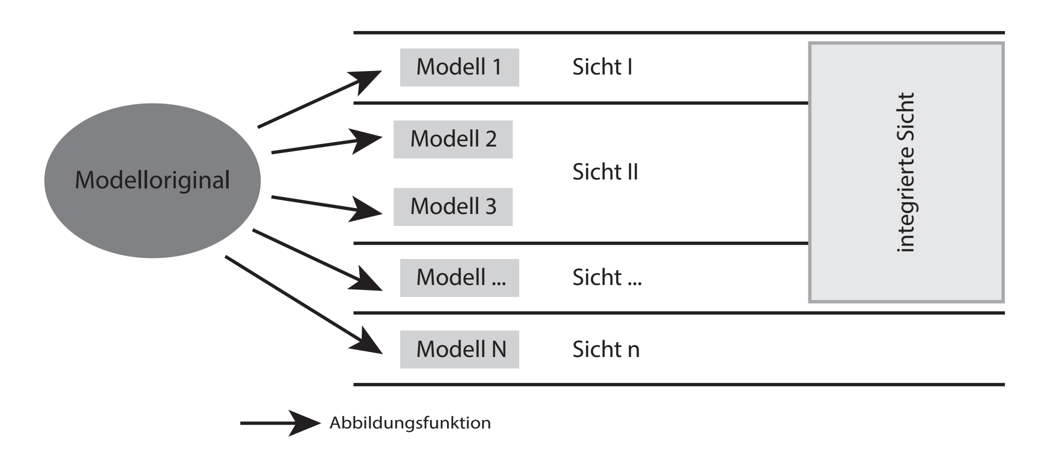


Abbildung 4: Zusammenhang Modelloriginal und Modell

Zur Veranschaulichung werden ein Flugzeug und verschiedene zugehörige Modelle betrachtet. Wahrscheinlich wurde während der Konstruktion des Flugzeuges ein digitales aerodynamisches Modell erstellt, und aerodynamische Eigenschaften wurden damit mittels einer IT-gestützten Simulation ermittelt. Zusätzlich wurde ein 3-D-Modell erstellt und im Windkanal getestet. Außerdem wurde neben dem eigentlichen Flugzeug auch ein Flugsimulator gebaut, um die Piloten für unerwartete, gefährliche Situationen zu trainieren. Aber auch für das Training der Kabinencrew kann ein weiteres Modell existieren, ein Kabinenmodell. Alle diese Artefakte sind Modelle, jedes Modell repräsentiert andere Aspekte des Flugzeuges. Die Modelle wurden für verschiedene Zwecke erstellt und sind verschiedene Sichten auf das gleiche Modelloriginal.

Skusa & Thalheim (Skusa & Thalheim, 2015, S. 431) beschreiben den Zusammenhang verschiedener Modelle bei der Modellierung von Informationssystemen. Unterschiedliche Aspekte von Informationssystemen werden getrennt voneinander betrachtet und modelliert. Dies führt zur Herausforderung, diese Modelle zu einem konsistenten Ganzen zusammenzuführen. Eine Lösung hierzu besteht darin, „mehrere Modelle zu einer modellübergreifenden Struktur, einer sogenannten Modell-Suite“ (Skusa & Thalheim, 2015, S. 435), zusammenzufassen.

Definition 4.2:
Modell-Suite
*Eine **Modell-Suite** „besteht aus*

- *einer Menge von Modellen $\{M_1, \dots, M_n\}$,*
- *Schemata für Assoziationen und Kollaborationen zwischen den Modellen,*
- *Controllern, welche für die Kohärenz der Modell-Suite sorgen,*
- *Bearbeitungsschemata, welche explizit die Bearbeitung und Weiterentwicklung der Modell-Suite beschreiben, und*
- *Tracern, mit denen sich die Herstellung von Kohärenz verfolgen lässt.“*

(Skusa & Thalheim, 2015, S. 436)

4.2 Sichten auf ein Unternehmen

Im Falle der Unternehmensmodellierung sind wie in Abbildung 5 dargestellt – neben anderen – die Sichten hinsichtlich Geschäftsprozess, Organisations-struktur und Datenstruktur relevant. Für die unterschiedlichen Sichten sind unterschiedliche Modelltypen notwendig. So werden Geschäftsprozesse beispielsweise in Petri-Netzen, die Organisationsstruktur beispielsweise in Organigrammen und die Datenstruktur in ER-Diagrammen beschrieben. Diese Modelle können dann, im Sinne einer Modell-Suite, miteinander verknüpft werden. Bevor die verschiedenen Sichten in den nachfolgenden Unterkapiteln genauer beschrieben werden, erfolgen erste Informationen auf die Werkzeugunterstützung und auf die durch diese Arbeit betrachtete Sicht der Informationssicherheit.

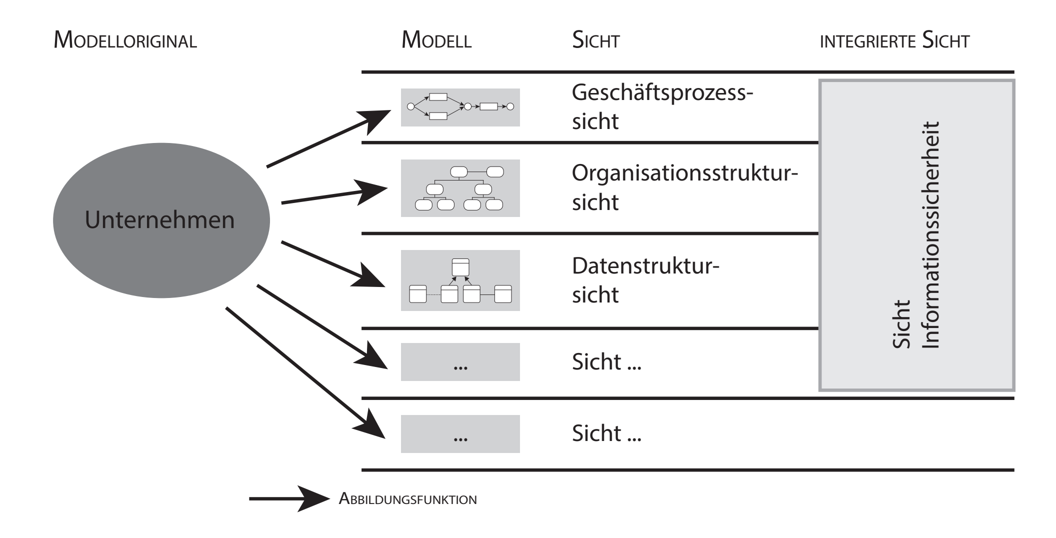


Abbildung 5: Sichten der Unternehmensmodellierung (vgl. Alpers, Pilipchuk, Oberweis & Reussner, 2018 S. 80, Abb. 1)

Zur Modellierung und zur Verknüpfung der unterschiedlichen Sichten wird in der Regel ein Modellierungswerkzeug verwendet. Beispielsweise unterstützt Horus[3] ein in

[3] www.horus.biz

Kooperation des Instituts für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) am Karlsruher Institut für Technologie (KIT) des Forschungsbereichs Software Engineering am FZI Forschungszentrum Informatik und des Industriepartners PROMATIS software GmbH entwickeltes Werkzeug (Schönthaler, Vossen, Oberweis & Karle, 2011, S. 6) die verschiedenen Modelltypen und ihre Verknüpfung. Das Werkzeug wird laufend weiterentwickelt, auch durch Prototypen, die bei den Forschungspartnern regelmäßig entstehen. Ein Beispiel dafür ist der mobile Petri-Netz-Editor (Alpers, Eryilmaz, Hellfeld & Oberweis, 2014).

Im Rahmen dieser Arbeit stehen Aspekte der Sicherheit im Fokus. Um Sicherheit durch Modellierung zu fördern, werden für bestimmte Arten von Modelloriginalen und bestimmte Modellierungssprachen Erweiterungen vorgenommen, um eine neue integrierte Sicht „Informationssicherheit“ zu generieren. Die Sicht Informationssicherheit baut als integrierte Sicht hierzu auf existierende Sichten der Unternehmensmodellierung auf und ergänzt die einzelnen Sichten und dazu notwendigerweise auch teilweise ihre Modellierungssprachen. Zusätzlich wird die Verknüpfung der verschiedenen Modelle formal definiert.

4.3 Die Geschäftsprozesssicht

In diesem Abschnitt werden zunächst verschiedene Definitionen des Begriffs Geschäftsprozess und verwandter und synonymer Begriffe untersucht, um anschließend eine Definition des Begriffs für diese Arbeit festzulegen.

Gadatsch (Gadatsch, 2015) definiert: Ein „Prozess ist eine sich regelmäßig wiederholende Tätigkeit mit einem definierten Beginn und Ende. Er verarbeitet Informationen (Input) zu zielführenden Ergebnissen (Output) und ist in der Regel arbeitsteilig organisiert. Er kann manuell, teilautomatisiert oder vollautomatisiert ausgeführt werden.“ Die Definition schränkt den „Input“ auf Informationen ein, ein Prozess kann darüber hinaus aber auch andere Ressourcen, wie beispielsweise Waren, verarbeiten.

Die Definition betont einen definierten Beginn und ein definiertes Ende eines Prozesses, lässt aber offen, ob es sich um eine einzelne oder mehrere sich regelmäßig wiederholende Tätigkeiten handelt. Da ein Prozess mehrere Tätigkeiten, aber – seltener – auch nur eine Tätigkeit umfassen kann, ist beides möglich.

Nach Oberweis (Oberweis, 1996, S. 15) können „Begriffe wie Geschäftsvorgang (-prozeß) , Business Process, Vorgangskette, Prozeßkette, Büroablauf (Office Procedure), Fertigungsablauf, verfahrenstechnischer Prozeß, Entwicklungsprozeß oder auch Workflow unter dem Oberbegriff betrieblicher Ablauf zusammengefasst“ werden. Er definiert den Begriff betrieblicher Ablauf hierzu wie folgt:

i. „Ein betrieblicher Ablauf ist eine Menge von manuellen, teilautomatisierten oder automatisierten Aktivitäten, die in einem Betrieb nach bestimmten Regeln auf ein bestimmtes Ziel hin ausgeführt werden. Die Aktivitäten hängen über betroffene Personen, Maschinen, Dokumente, Betriebsmittel u. ä. miteinander zusammen.
ii. Aktivitäten werden durch sogenannte Aufgabenträger ausgeführt. Es wird zwischen personellen und nichtpersonellen (maschinellen) Aufgabenträgern unterschieden […]. Aufgaben sind hier als zu erbringende Leistungen zu verstehen, wobei die Erfüllung einer Aufgabe durch Ausführung einer oder mehrerer Aktivitäten erfolgt.
iii. Ein kooperativer oder arbeitsteiliger (betrieblicher) Ablauf ist dadurch gekennzeichnet, daß mindestens zwei Aufgabenträger seine Aktivitäten ausführen.
iv. Ein verteilter (betrieblicher) Ablauf liegt dann vor, wenn (mindestens zwei) Aktivitäten eines (betrieblichen) Ablaufs an geographisch unterschiedlichen Orten ausgeführt werden.“

- (Oberweis, 1996, S. 14f.)

Dabei versteht Oberweis (Oberweis, 1996, S. 14) unter einem Betrieb „auch zum Beispiel Dienstleistungsunternehmen, Krankenhäuser, Behörden u. ä.“. Gemäß dieser Definition ist der Ausführungsort „im Betrieb“ für die Einordnung als betrieblicher

Ablauf entscheidend. Dadurch wird der Charakter des Oberbegriffs deutlich, der verschiedene Untergliederungen des Begriffs Prozess umfasst. So untergliedert Berkau (Berkau, 1998) den Begriff Prozess in technische Prozesse und (betriebswirtschaftliche) Geschäftsprozesse.

Werden Prozesse zur betrieblichen Aufgabenerfüllung gestaltet, sei es zur direkten Wertschöpfung oder als Unterstützung, werden diese Prozesse in dieser Arbeit als Geschäftsprozesse bezeichnet. In Anlehnung an Oberweis (Oberweis, 1996) wird nachfolgend der Begriff Geschäftsprozess definiert.

Definition 4.3:
Geschäftsprozess

- *Ein **Geschäftsprozess** ist eine Menge von manuellen, teilautomatisierten oder automatisierten Aktivitäten (Tätigkeiten), die nach bestimmten Regeln ausgeführt werden. Mit der Ausführung wird die Erreichung eines bestimmten unternehmerischen Zieles angestrebt.*
- *Von den Aktivitäten können Objekte erzeugt, konsumiert, benötigt oder bearbeitet werden. Objekte können beispielsweise Rohstoffe, Fertigungsstücke, aber auch Informationen sein.*
- *Die Aktivitäten werden durch personelle und/oder nichtpersonelle Ressourcen ausgeführt.*
- *Ein Geschäftsprozess ist arbeitsteilig, wenn mindestens zwei Ressourcen seine Aktivitäten ausführen.*
- *Ein Geschäftsprozess ist unternehmens- beziehungsweise organisationsübergreifend, wenn mindestens zwei Unternehmen beziehungsweise Organisationen an der Ausführung der Aktivitäten beteiligt sind.*

Analog zur Verwendung des Begriffs Betrieb bei Oberweis (Oberweis, 1996, S. 14) schließen unternehmerische Ziele auch Ziele von Organisationen, wie Krankenhäusern, Behörden und gemeinnützigen Organisationen (zum Beispiel Stiftungen und Vereinen), mit ein.

Von einem Geschäftsprozess ist die modellhafte Darstellung desselben zu unterscheiden. Unabhängig von einer solchen modellhaften Darstellung kann ein Geschäftsprozess beispielsweise während der Ausführung einer Instanz durch die beteiligten Ressourcen beobachtet werden (Gadatsch, 2015).

Definition 4.4:
Geschäftsprozessmodell

- *Die modellhafte Darstellung eines Geschäftsprozesses als Modell heißt **Geschäftsprozessmodell** oder Geschäftsprozessschema.*

Die Geschäftsprozessmodellierung ist ein Teil der Unternehmens-modellierung. Mithilfe der Geschäftsprozessmodellierung kann das Verhalten eines Unternehmens modelliert werden. Andere Bereiche der Unternehmens-modellierung betrachten beispielsweise auch statische Aspekte wie die Organisationsstruktur. Da jedoch in der Geschäftsprozessmodellierung insbesondere dynamische, aktivitätsbezogene Aspekte betrachtet werden, ist es wichtig, die Begriffe Geschäftsprozess, Geschäftsprozessmodell und Geschäftsprozessinstanz zu unterscheiden (Gadatsch, 2015).

Definition 4.5:
Geschäftsprozessinstanz

- *Eine **Geschäftsprozessinstanz** bezeichnet einen konkreten Geschäftsvorgang, das heißt eine konkrete Durchführung beziehungsweise Ausprägung eines Geschäftsprozesses.*

Können beispielsweise in einem Geschäftsprozessmodell Ressourcen und verarbeitete Objekte nur bezüglich ihrer Typen festgelegt werden, werden in einer Geschäftsprozessinstanz vor oder während der Ausführung Ressourcen und Objekte konkretisiert. Zwei Geschäftsprozessinstanzen des gleichen Geschäftsprozessmo-

dells unterscheiden sich oft hinsichtlich der verwendeten Objekte. Eventuell unterscheiden sich sogar die ausgeführten Aktivitäten, wenn das Geschäftsprozessmodells hier Alternativen vorsieht.

4.3.1 Petri-Netze

In diesem Abschnitt werden ausgewählte Grundlagen zur Modellierungssprache Petri-Netze zur Modellierung von Geschäftsprozessen erläutert, weil die in dieser Arbeit vorgestellten Sicherheitsnetze eine Erweiterung der Petri-Netze darstellen.

Petri-Netze sind eine Struktur mit zwei Sorten von Elementen: Stellen und Transitionen. Diese werden durch Kanten miteinander verbunden (Reisig, 2010):

- Stellen bilden die passiven Komponenten von Petri-Netzen und dienen i. d. R. zur Modellierung von Zuständen. Zusätzlich können Stellen Dinge lagern und Informationen speichern. Stellen werden in dieser Arbeit als Kreis dargestellt. Ein gebräuchliches Synonym für Stellen sind Plätze.
- Aktivitäten, als zentrales Element der Geschäftsprozessmodellierung, werden in Petri-Netzen als Transitionen abgebildet. Diese werden in dieser Arbeit mit einem Rechteck dargestellt.
- Der Kontrollfluss als wesentliche Möglichkeit, die Regeln eines Geschäftsprozesses abzubilden, wird als gerichtete Kante dargestellt.



Abbildung 6: Symbole für Stelle, Transition und gerichtete Kante

Neben dieser grafischen Darstellungsnotation besitzen Petri-Netze eine mathematische Fundierung und können entsprechend definiert werden (W. van der Aalst & Stahl, 2011, S. 73; vgl. Reisig, 1986, S. 16; Reisig, 2010, S. 23):

Definition 4.6:
Petri-Netz
Ein ***Petri-Netz*** *ist ein Tupel* $N = (P, T, F)$ *mit*
1. P *als eine endliche Menge von Stellen.*
2. T *als eine endliche Menge von Transitionen.*
3. $P \cap T = \emptyset$.
4. $F \subseteq (P \times T) \cup (T \times P)$ *als eine Flussrelation.*

Die Bedingung der Flussrelation (4) garantiert, dass es keine direkte Verbindung von Stellen zu Stellen beziehungsweise von Transitionen zu Transitionen gibt. Relationen sind nur zwischen Transitionen und Stellen und umgekehrt zulässig. Die gerichteten Kanten gehen also immer von einer Stelle zu einer Transition oder umgekehrt.

Objekte (siehe Definition 4.3) werden in Petri-Netzen durch Marken dargestellt. Marken können aber nicht nur Objekte repräsentieren, sondern auch nur dazu dienen, den Kontrollfluss zu steuern. Für Marke wird oft das Synonym Token gebraucht. Die Verteilung aller Marken, das heißt die Belegung der Stellen durch Marken, in einem Petri-Netz wird als Markierung des Petri-Netzes (W. van der Aalst & Stahl, 2011) bezeichnet. Die Markierung enthält somit den Zustand des Netzes. Sie lässt sich nach van der Aalst & Stahl (W. van der Aalst & Stahl, 2011, S. 77) wie folgt definieren:

Definition 4.7:
Markierung eines Petri-Netzes

- *Eine **Markierung** m **eines Petri-Netzes** $N = (P, T, F)$ ist eine Funktion $m : P \rightarrow \mathbb{N}$, die jeder Stelle $p \in P$ die Anzahl der Marken in dieser Stelle zuordnet.*
- *Die Menge M enthält alle Markierungsfunktionen eines Petri-Netzes.*

Aufgrund einer Markierung kann bestimmt werden, ob eine Transition schalten kann. Dazu müssen zunächst der Vor- und der Nachbereich einer Transition definiert werden (W. van der Aalst & Stahl, 2011, S. 73).

Definition 4.8:
Vor- und Nachbereich einer Transition in einem Petri-Netz $\boldsymbol{N} = (\boldsymbol{P}, \boldsymbol{T}, \boldsymbol{F})$

- *Eine Stelle p ist eine Eingangsstelle einer Transition t genau dann, wenn $(p, t) \in F$.*
- *Die Menge $\bullet t = \{p \mid (p, t) \in F\}$ definiert den Vorbereich einer Transition t.*
- *Eine Stelle p ist eine Ausgangsstelle einer Transition t genau dann, wenn $(t, p) \epsilon F$.*
- *Die Menge $t \bullet = \{p \mid (t, p) \in F\}$ definiert den Nachbereich einer Transition t.*

Dies lässt sich auch auf den Vor- und Nachbereich einer Stelle übertragen.

Definition 4.9:
Vor- und Nachbereich einer Stelle in einem Petri-Netz $\boldsymbol{N} = (\boldsymbol{P}, \boldsymbol{T}, \boldsymbol{F})$

- *Die Menge $\bullet p = \{t \mid (t, p) \in F\}$ definiert den Vorbereich einer Stelle p.*
- *Die Menge $p \bullet = \{t \mid (p, t) \in F\}$ definiert den Nachbereich einer Stelle p.*

Nun kann bestimmt werden, ob eine Transition schalten kann, das heißt aktiviert ist. Dazu muss sich in jeder Stelle des Vorbereiches mindestens eine Marke befinden. Falls dies der Fall ist, kann eine Transition schalten. Wenn eine Transition schaltet, wird aus jeder Stelle des Vorbereichs eine Marke entnommen (das heißt, die Marke wird konsumiert), und in jeder Stelle des Nachbereichs wird eine neue Marke erzeugt. Formal lässt sich diese Schaltregel nach van der Aalst & Stahl (W. van der Aalst & Stahl, 2011, S. 77f.) wie folgt definieren:

Definition 4.10:
Schaltregel

- *In einem Petri-Netz $N = (P, T, F)$ ist eine Transition $t \in T$ genau dann unter einer Markierung $m : P \rightarrow \mathbb{N}$ aktiviert, wenn für alle $p \in \bullet t$ gilt: $m(p) > 0$.*
- *Eine aktivierte Transition kann schalten.*
- *Wenn eine Transition $t \in T$ schaltet, wird die Markierung $m : P \rightarrow \mathbb{N}$ in die Markierung $m' : P \rightarrow \mathbb{N}$ überführt. m' lässt sich wie folgt berechnen:*
  für alle $p \in P$: $m'(p) = m(p) - w\big((p, t)\big) + w((t, p))$
  $w: (P \times T) \cup (T \times P) \rightarrow \{0, 1\}$ mit $w\big((x, y)\big) = 1$ wenn $(x, y) \in F$ und $w\big((x, y)\big) = 0$ wenn $(x, y) \notin F$.

Abbildung 7 zeigt ein Petri-Netz mit zwei Stellen und einer Transition. Das Petri-Netz hat zunächst eine Startmarkierung (links in der Abbildung). Dadurch ist die Transition aktiviert und kann schalten. Beim Schalten der Transition wurde die Marke aus der Eingangsstelle konsumiert und eine Marke in der Ausgangsstelle erzeugt. Das Resultat ist rechts in der Abbildung zu sehen.



Abbildung 7: Petri-Netz vor (links) und nach (rechts) Schalten der Transition

Die gerichteten Kanten bestimmten die möglichen Ausführungsreihenfolgen der Aktivitäten. Aktivitäten können sequenziell, alternativ oder nebenläufig stattfinden. Die einzelnen Fälle sind nachfolgend gemäß van der Aalst & Stahl (W. van der Aalst & Stahl, 2011) beschrieben und in Abbildung 8 dargestellt.

- Im Falle einer sequenziellen Ausführung der Aktivitäten x und y muss die eine Aktivität abgeschlossen sein, bevor die andere Aktivität beginnen kann. Im Fall x vor y muss also x zuerst zu Ende sein und erst danach kann y beginnen.
- Falls entweder x oder y ausgeführt werden soll, spricht man von einer alternativen Ausführung. Möglich ist auch, zu bestimmen, dass danach z ausgeführt werden soll.
- Wenn die Aktivitäten x und y keine kausale Beziehung zueinander haben und beide ausgeführt werden sollen, so können diese nebenläufig ausgeführt werden. Da x und y dann voneinander unabhängig sind, kann entweder zuerst x und dann y stattfinden oder umgekehrt. Es ist auch möglich, dass beide zu einem Zeitpunkt stattfinden. Im Extremfall beginnen und enden sie jeweils gleichzeitig, das heißt in einem Schritt. Es ist aber auch möglich, dass sich x und y nur überlappen (x beginnt, y beginnt, x endet, y endet) oder dass x beginnt und endet, während y ausgeführt wird (y beginnt, x beginnt, x endet, y endet) (Oberweis, 1990). Soll z ausgeführt werden, nachdem x und y fertig ausgeführt wurden, ist eine Synchronisation erforderlich.

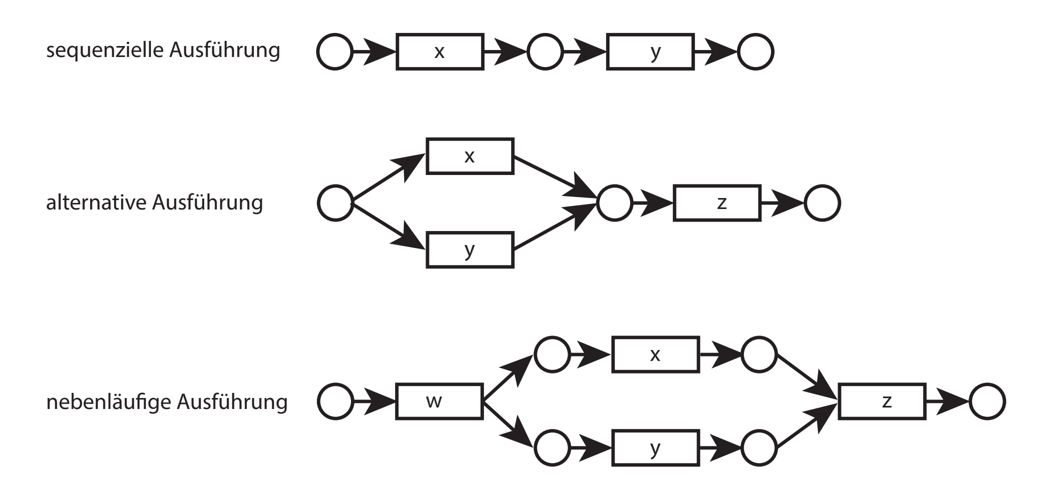


Abbildung 8: Sequenzielle, alternative und nebenläufige Ausführung in Petri-Netzen

Für Petri-Netze ist der Begriff des Pfades wichtig. Ein Pfad beschreibt den Weg von einem Knoten zu einem anderen Knoten über Kanten des Petri-Netzes.

> *Definition 4.11:*
> *Pfad*
> *Sei N ein Petri-Netz $N = (P, T, F)$, so ist P ein* ***Pfad*** *vom Knoten n_1 zum Knoten n_k (ein Knoten kann eine Stelle oder eine Transition sein) eine Folge (Sequenz) $(n_1, n_2, \ldots, n_k)$, sodass $(n_i, n_{i+1}) \in F$ für $1 \leq i \leq k-1$.*

Seit der Erfindung von Petri-Netzen sind viele Arbeiten dazu entstanden. Ein Beispiel dafür ist die Unterscheidbarkeit von Marken. In den ursprünglichen Petri-Netzen werden nur nicht unterscheidbare, gleichartige Marken verwendet. Die Unterscheidbarkeit, das heißt individuelle Marken, ist inzwischen mit gefärbten Petri-Netzen (Jensen, 1987) und XML-Netzen (Lenz & Oberweis, 2003) gegeben.

4.3.2 Workflow-Netze

Weitere Analysemöglichkeiten entstehen, wenn statt allgemein Petri-Netze speziell Workflow-Netze betrachtet werden. Nach van der Aalst & van Hee (W. van der Aalst & van Hee, 2004) ist der Begriff Workflow in diesem Fall ein Synonym für Geschäftsprozess. Workflow-Netze sind eine Teilmenge der Petri-Netze. Jedes Workflow-Netz muss nach van der Aalst (W. M. van der Aalst, 1998) über eine Quelle und eine Senke verfügen. Eine Quelle (auch Input-Stelle genannt) ist eine Stelle, die einen leeren Vorbereich hat, eine Senke (auch Output-Stelle genannt) ist eine Stelle mit einem leeren Nachbereich. Zusätzlich darf es keine Transition und keine Stelle geben, die nicht zur Verarbeitung von Geschäftsvorfällen beitragen kann. Das bedeutet, jede Stelle und jede Transition muss auf mindestens einem Pfad von der Quelle zur Senke liegen. Um die letzte Bedingung auszudrücken, nutzt van der Aalst (W. M. van der Aalst, 1998) die Eigenschaft „streng zusammenhängend“, die einige Petri-Netze besitzen. Sie lässt sich wie in Definition 4.12 formal definieren (W. M. van der Aalst, 1998).

Definition 4.12:
streng zusammenhängend
*Ein Petri-Netz $N = (P, T, F)$ ist **streng zusammenhängend**, wenn für jedes Knotenpaar x und y ein Pfad von x nach y existiert.*

Workflow-Netze sind nicht streng zusammenhängend. Dies ist auch darin begründet, dass Geschäftsprozesse in der Regel von einer Quelle zu einer Senke führen. Eine Bedingung von Workflow-Netzen ist aber, dass das um eine Transition t^* erweiterte Workflow-Netz streng zusammenhängend ist. Dabei muss die Senke des Workflow-Netzes der Vorbereich von t^* und die Quelle der Nachbereich von t^* sein. Damit lässt sich nun ein Workflow-Netz formal definieren. Van der Aalst (W. M. van der Aalst, 1998) beschreibt dies wie in Definition 4.13.

Definition 4.13:
Workflow-Netz
*Ein Petri-Netz $N = (P, T, F)$ ist ein **Workflow-Netz** $WF = (P, T, F)$, wenn und nur wenn:*

- *WF zwei spezielle Stellen hat:*
  - i ist eine Quelle, es gilt: $\bullet i = \emptyset$
  - o ist eine Senke, es gilt: $o \bullet = \emptyset$
- *Wenn eine Transition t^* zum Petri-Netz N hinzugefügt wird, sodass die Stelle o mit der Stelle i verbunden wird $\left(\bullet t^* = \{o\} \wedge t^* \bullet = \{i\}\right)$, dann ist das resultierende Petri-Netz streng zusammenhängend.*

4.3.3 Analysemethoden für Petri-Netze

Petri-Netze wurden unter anderem wegen der mathematischen Eigenschaften und der damit verbundenen Analysemöglichkeiten für die Sicherheitsnetze ausgewählt. Einige untersuchbare Eigenschaften werden nachfolgend vorgestellt.

Eine wichtige Eigenschaft ist die **Erreichbarkeit** einer Markierung $m' \in M$ von einer Markierung $m \in M$ aus. Nach van der Aalst & Stahl (W. van der Aalst & Stahl, 2011, S. 76) lässt sich Erreichbarkeit wie folgt definieren:

Definition 4.14:
Erreichbarkeit
Eine Markierung $m' \in M$ ist von einer Markierung $m \in M$ aus erreichbar, wenn eine Schaltfolge von m zu m' existiert.

Zusätzlich lässt sich dann die Erreichbarkeitsmenge $\mathcal{E}(m)$ definieren (Priese & Wimmel, 2008, S. 52).

Definition 4.15:
Erreichbarkeitsmenge
*Die **Erreichbarkeitsmenge** $\mathcal{E}\ (m)$ ist die Menge aller Markierungen, die von der Markierung $m \in M$ aus erreichbar sind.*

Zu einer Markierung m kann die Erreichbarkeitsmenge mittels eines Erreichbarkeitsgraphen ermittelt werden. Die Knoten repräsentieren die erreichbaren Markierungen. Jede gerichtete Kante zwischen den Knoten repräsentiert eine Transition, die das Netz von einem Zustand in einen anderen Zustand überführt. Bei komplexeren Petri-Netzen, ggf. sogar mit mehreren Marken in einer Markierung, kann das Erstellen des Erreichbarkeitsgraphen aufwendig sein. Es gibt auch Fälle, in denen der Erreichbarkeitsgraph unendlich viele Knoten hat. Der Erreichbarkeitsgraph kann algorithmisch berechnet werden (W. van der Aalst & Stahl, 2011, S. 115ff.). Zusätzlich gibt es weitere Analysemöglichkeiten beziehungsweise Eigenschaften für Workflow-Netze.

5 Informationsvertraulichkeits- und Datenschutz-Netze

Im nachfolgenden Kapitel werden Aspekte der Informationssicherheit und des Datenschutzes in die Unternehmensmodellierung integriert. Einen Schwerpunkt bildet die Modellierung von Geschäftsprozessen (das heißt der betrieblichen Ablauforganisation) mittels Petri-Netzen[1]. Jedoch können weder Informationssicherheit noch Datenschutz ausschließlich innerhalb der Ablauforganisation hinreichend betrachtet werden. Weitere Aspekte aus der Aufbauorganisation und den Datenstrukturen werden daher in die Modellierung integriert. So entsteht eine neue, umfassende und integrierende Sicht.

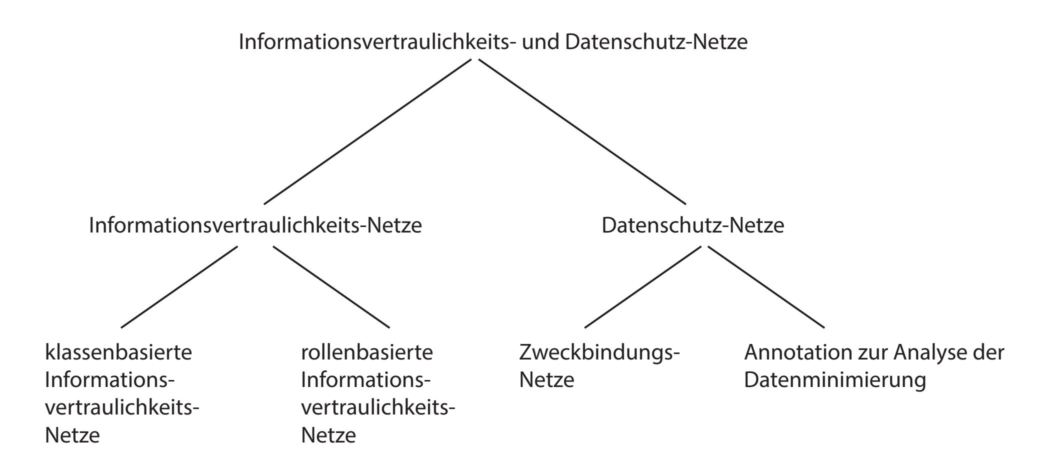


Abbildung 9: Übersicht der verschiedenen Netze

Die verschiedenen Netze, welche zunächst entwickelt und anschließend zu Informationsvertraulichkeits- und Datenschutz-Netzen zusammengeführt werden, sind in

[1] Genauer gesagt wird auch die Unterscheidbarkeit von Marken, eine Eigenschaft von höheren Petri-Netzen, benötigt.

Abbildung 9 dargestellt. Zunächst wird im ersten Unterkapitel *Informationsvertraulichkeit* als Aspekt der Informationssicherheit betrachtet, danach werden die Grundsätze der *Zweckbindung* und der *Datenminimierung* aus dem Datenschutzrecht im zweiten Unterkapitel behandelt. Anschließend werden die Betrachtungen in einem neuen, die verschiedenen Aspekte umfassenden *Informationsvertraulichkeits- und Datenschutz-Netz* integriert.

5.1 Informationsvertraulichkeit

Informationen haben eine Schlüsselrolle bei der Ausführung von Geschäftsprozessen. Dies schließt Informationen, die bereits vor der Geschäftsprozessausführung existieren, genauso ein wie Informationen, die während der Geschäftsprozessausführung erzeugt werden. Dabei gibt es in der Regel Anforderungen an die Informationsvertraulichkeit. Die Notwendigkeit der Sicherstellung der Informationsvertraulichkeit kann sich u. a. aufgrund von Gesetzen, organisationsfremden und eigenen Richtlinien oder wirtschaftlichen Interessen ergeben. Dabei muss nicht unbedingt zwischen Geschäfts- und Betriebsgeheimnissen unterschieden werden. Geschäftsgeheimnisse stammen aus der „kaufmännisch-geschäftlichen Sphäre des Unternehmens“ (Müller, 2013, S. 119) und Betriebsgeheimnisse aus den „technischen Betriebsabläufen“ (Müller, 2013, S. 119). Beide Typen können nach Müller (Müller, 2013, S. 119) einen erheblichen Unternehmenswert darstellen.

Um Informationsvertraulichkeit zu erreichen, muss die „unautorisierte Informationsgewinnung“ verhindert werden (Eckert, 2018, S. 10). Um diese Anforderung in der Unternehmensmodellierung zu berücksichtigen, muss man unautorisierten von autorisiertem Informationsgewinn je Information unterscheiden. Betrachtet man keine Geschäftsprozessinstanzen, sondern Geschäftsprozessmodelle, muss diese Unterscheidung für Informationstypen vorgenommen werden.

Es bedarf dazu zunächst einer Festlegung, welche Ressourcen welche Informationen beziehungsweise Informationstypen autorisiert gewinnen dürfen. Ressourcen können dabei sowohl Menschen und Organisationen als auch IT-Systeme sein. Menschen können prozessbeteiligte Mitarbeiter des Unternehmens oder der Organisation selbst, aber auch Angehörige dritter Organisationen oder Privatpersonen sein.

Eventuell kennt der Prozessmodellierer beispielsweise im Falle einer weisungsgebundenen Auftragsverarbeitung die ausgelagerten Prozessschritte und die beteiligten Ressourcen innerhalb von dritten Organisationen einzeln und kann diese wie interne Prozessschritte auch modellieren. Es kann aber auch sein, dass dem Prozessmodellierer ggf. die internen Prozessschritte und die damit verbundene Informationsgewinnung innerhalb dieser dritten Organisationen nicht bekannt sind; somit muss es möglich sein, diese Organisationen im Ganzen als eine Ressource und ihre Tätigkeit zwischen zwei internen Prozessschritten ggf. auch als einen einzelnen Prozessschritt zu betrachten. Auch IT-Systeme können Informationen gewinnen und müssen daher ebenfalls als möglicherweise informationsgewinnende Ressource im Nachfolgenden berücksichtigt werden.

Gleichzeitig ist nicht jede Information überhaupt vertraulich. So gibt es beispielsweise öffentliche Informationen, die jedem bekannt sind beziehungsweise bekannt sein dürfen. Ein Beispiel sind die im Katalog veröffentlichten Preise für verschiedene Produkte des Unternehmens. Für vertrauliche Informationen (im obigen Beispiel der Katalogpreise evtl. die Kalkulation der Katalogpreise) ist der Kreis der autorisierten Ressourcen festzulegen. Hierzu werden im Folgenden zwei Möglichkeiten vorgestellt. Zum einen die Einstufung in Vertraulichkeitsklassen und zum anderen ein rollenbasiertes Vorgehen. Beide Möglichkeiten können später auch mit weiteren Zugriffsbeschränkungen, beispielsweise in Abhängigkeit des Ausführungsortes oder der Zeit, kombiniert werden (vgl. Decker, 2011; Schiefer, 2015).

5.1.1 Klassenbasierte Informationsvertraulichkeit

Die Klassifikation von einzelnen Elementen mit dem Ziel, Sicherheitsanforderungen durchzusetzen, ist in der Sicherheitsforschung weit verbreitet. Eine der ersten Arbeiten hierzu ist das Bell-LaPadula-Modell (Bell & LaPadula, 1976), welches Elemente von Informationssystemen sowie Mechanismen, Regeln und Sicherheitsklassifikationen für Zugriffssteuerungen beschreibt (McLean, 1985). Auch in der Praxis wird die Klassifikation von Informationen zu ihrem Schutz eingesetzt. So gaben in der neusten <kes>/Microsoft-Sicherheitstudie 83 Prozent der Befragten an, dass in ihrem Unternehmen „eine Klassifikation von Daten hinsichtlich ihrer Sensibilität" erfolgt (<kes>, 2018, S. 64).

Für die Klassifikation von Informationsvertraulichkeit wird im Rahmen des vorliegenden Lösungsansatzes eine Ordinalskala verwendet (vgl. Landwehr, Heitmeyer & McLean, 1984). Mittels der Ordinalskala ist es möglich, Information basierend auf ihrer Sensibilität zu klassifizieren - je höher die Klasse einer Information, desto vertraulicher ist die Information. Eine beispielhafte Ordinalskala für den Einsatz im Unternehmen wird in Tabelle 2 beschrieben. Die Klasse 0 wird vergeben, wenn es sich um eine nicht vertrauliche Information (das heißt eine Information, die der Öffentlichkeit bekannt sein darf) handelt. Die aufsteigenden Klassen von 1 bis 4 stehen jeweils für entsprechende Informationsvertraulichkeitsklassen. Die Klasse 4 wird nur für Informationen vergeben, die der höchsten Geheimhaltungsstufe im Unternehmen unterliegen.

Tabelle 2: Ordinalskala für die Informationsvertraulichkeitsklassifikation

Informations-Vertraulichkeits-klasse	Beschreibung
0	frei zugänglich: Die Information darf der Allgemeinheit zugänglich sein. Zum Beispiel ein Jahresbericht auf der Webseite eines Unternehmens.
1	beschränkt: Die Information darf an Dritte weitergegeben werden, wenn eine entsprechende vertragliche Vereinbarung den Schutz der Information regelt. Ein typisches Beispiel ist eine Konstruktionszeichnung eines Teils einer Produktionsmaschine, die im Rahmen einer bestehenden und vertraglich geregelten Kooperation zweier Unternehmen ausgetauscht wird.
2	vertraulich: Die Information darf nur unternehmensintern verwendet werden, beispielsweise sensible Informationen über einen einzelnen Kunden.
3	geheim: Die Information ist nur einem spezifischen Personenkreis zugänglich, beispielsweise strategische Informationen über Teile des Geschäftsmodells eines Unternehmens wie Selbstkosten eines Produktes. Ein anderes Beispiel wären Konstruktionszeichnungen eines zukünftigen Produktes.
4	streng geheim: Die Anzahl der Personen, die Zugriff auf die Information besitzen, ist sehr gering, beispielsweise Informationen, die den Fortbestand eines Unternehmens bei Zugriff durch Dritte (Konkurrenten, Öffentlichkeit) unmittelbar gefährden könnten.

Um nun festlegen zu können, welche Ressourcen autorisiert sind, eine klassifizierte Information zur Kenntnis zu nehmen, ist eine Einstufung der Ressourcen in passende Vertrauenswürdigkeitsklassen notwendig. Vertrauenswürdigkeit betrachtet nach Hardin (Hardin, 2002) das Ergebnis der Einschätzung einer Ressource hinsichtlich der Frage, ob die Ressource sich so verhalten wird, wie das Vertrauen eines Dritten in die Ressource es erfordert.

Tabelle 3: Ordinalskala für die Vertrauenswürdigkeitsklassifikation von Ressourcen

Vertrauens-würdigkeits-klasse	Beschreibung
0	nicht vertrauenswürdig: beispielsweise eine externes IT-System in einer unsicheren Umgebung oder eine Person mit schweren finanziellen Schwierigkeiten (und dadurch bedingter starker Anfälligkeit für Korruption).
1	gering vertrauenswürdig: beispielsweise eine unternehmensexterne Ressource, mit der eine vertragliche, jedoch nur zivilrechtlich durchsetzbare Vereinbarung besteht. Dies kann eine ganze Organisation oder auch nur ein einzelner Mitarbeiter beziehungsweise ein einzelnes System sein.
2	vertrauenswürdig: beispielsweise eine unternehmensexterne Ressource, bei der vertrags- und strafrechtliche Durchsetzungsmöglichkeiten der Vereinbarung bestehen, oder eine unternehmensinterne Ressource.
3	stark vertrauenswürdig: beispielsweise eine unternehmensinterne Person, bei der vertrags- und strafrechtliche Durchsetzungsmöglichkeiten der Vereinbarung bestehen, oder eine unternehmensinterne Maschine mit speziellen Schutzmechanismen (zum Beispiel vollständige Verschlüsselung).
4	besonders vertrauenswürdig: beispielsweise Personen mit einer intrinsischen Motivation zum Schutz der Informationsvertraulichkeit.

Vertrauenswürdigkeit ist folglich eine Eigenschaft einer Ressource, das heißt einer Person oder eines Systems[2]. Zur Klassifizierung der Vertrauenswürdigkeit von Ressourcen wird eine weitere Ordinalskala verwendet (eine mögliche Skala ist in Tabelle 3 dargestellt). Da eine Ressource bis zu ihrer Klassifikation keinerlei Zugriff auf vertrauliche Informationen erhalten darf, ist der initiale Wert 0. Die Klasse 0 steht dafür, dass eine Ressource überhaupt nicht vertrauenswürdig ist. Folglich darf sie (ggf. bis zu einer Erstklassifizierung beziehungsweise Reklassifizierung aufgrund veränderter

[2] In dieser Arbeit werden sowohl Personen als auch Systeme wie beispielsweise ein Server oder ein Softwaresystem als Ressource betrachtet. Personen können entweder konkrete natürliche Personen oder Organisationen bzw. Organisationseinheiten sein.

Umstände) keinen Zugriff auf vertrauenswürdige Informationen erhalten. Je höher die Klassifikation, desto vertrauenswürdiger ist die Ressource.

Um darauf aufbauend nun klassifikationsbasierte Informationsvertraulichkeit in Geschäftsprozessmodellen beschreiben, betrachten und analysieren zu können, werden daher neben dem Geschäftsprozessmodell auch die Verknüpfungen zu Ressourcenmodellen (zwecks Betrachtung der Vertrauenswürdigkeit) und Objektmodellen (zwecks Betrachtung der Informationsvertraulichkeit) beachtet. Um die Analyse eines Geschäftsprozessmodells hinsichtlich Informationsvertraulichkeit zu vereinfachen, werden existierende Petri-Netze mit den oben beschriebenen Artefakten zu den sogenannten klassenbasierten Informationsvertraulichkeits-Netzen (cICN) erweitert, siehe Definition 5.1:

Definition 5.1:
klassenbasiertes Informationsvertraulichkeits-Netz
Ein ***klassenbasiertes Informationsvertraulichkeits-Netz*** *ist ein Tupel* $cICN = (P, T, F, R, I, IT, RT, ITP, C, CT, TW)$ *mit*

- P *als eine endliche Menge von Stellen,*
- T *als eine endliche Menge von Transitionen,*
- $P \cap T = \emptyset$,
- $F \subseteq (P \times T) \cup (T \times P)$ *als eine Flussrelation,*
- R *als eine endliche Menge von Ressourcen,*
- I *als eine Menge von Informationsobjekten,*
- IT *als eine Menge von Informationsobjekttypen,*
- $RT \subseteq (\mathcal{P}(R) \times T)$ *als eine Allokation von Ressourcen zu Transitionen,*
- $ITP \subseteq (\{IT \cup \emptyset\} \times P)$ *als eine Allokation von jeweils keinem oder einem Informationsobjekttypen zu einer Stelle,*
- $C: I \rightarrow \mathbb{N}$ *als die Informationsvertraulichkeit der Information,*
- $CT: IT \rightarrow \mathbb{N}$ *als die Informationsvertraulichkeit des Informationsobjekttyps und*
- $TW: R \rightarrow \mathbb{N}$ *als die Vertrauenswürdigkeit einer Ressource r.*

Das Beispiel aus Tabelle 2 zugrunde gelegt, gilt für die Informationsvertraulichkeit $C: I \rightarrow \{0,1,2,3,4\}$, und für die Vertrauenswürdigkeit gilt nach Tabelle 3 entsprechend $TW: R \rightarrow \{0,1,2,3,4\}$. Zur Veranschaulichung zeigt Abbildung 10 einen Ausschnitt aus einem klassenbasierten Informationsvertraulichkeits-Netz. Die Menge der Stellen umfasst im abgebildeten Ausschnitt {p5, p6, p7}, die Menge der Transitionen {Kartendaten speichern, Kartendaten kürzen}. Die Ressourcen sind rot hervorgehoben, und in Klammern ist bereits jeweils ihre Vertrauenswürdigkeit angegeben, die Menge ist hier {Zahlungssystem, Kartenbesitzer}. Dementsprechend ist TW(Zahlungssystem)=4 und TW(Kartenbesitzer)=3. Mit der Transition Kartendaten speichern sind beide Ressourcen verknüpft, mit der Transition Kartendaten kürzen ist nur die Ressource Zahlungssystem verknüpft. Da noch keine Markierung angegeben ist, sind keine Informationsobjekte zu sehen. Die Menge der Informationsobjekttypen ist in dem Ausschnitt grün dargestellt {Zahlungsdaten, Zahlmittelübersicht}. Ihre jeweilige Informationsvertraulichkeit ist in Klammern angegeben: CT(Zahlungsdaten)=3 und CT(Zahlmittelübersicht)=1. Die Allokationen RT und ITP sind grafisch zu erkennen.

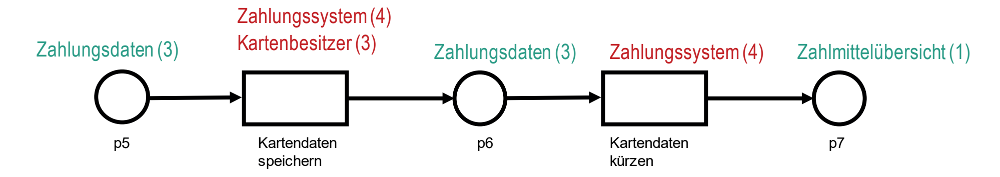


Abbildung 10: beispielhafter Ausschnitt eines einfachen klassenbasierten Informationsvertraulichkeits-Netzes

Die Markierung eines klassenbasierten Informationsvertraulichkeits-Netzes ist durch Definition 5.2 konkretisiert. Die Marken sind jeweils Informationsobjekte, für die Modellierung eines reinen Kontrollflusses wird ein leeres Informationsobjekt verwendet. Das bedeutet, dass in jeder Stelle keines, eines oder mehrere Informationsobjekte der aus der Menge I liegen. Dementsprechend werden die Stellen P auf die Potenzmenge von I abgebildet.

Definition 5.2:
Markierung eines klassenbasierten Informationsvertraulichkeits-Netzes
Die ***Markierung*** *eines klassenbasierten Informationsvertraulichkeits-Netzes $cICN$ ist definiert als*

- $m: P \rightarrow \mathcal{P}(I)$.

Die Menge M ist die Menge der Markierungen.

Nachfolgend werden zwei Hauptmerkmale von Informationsvertraulichkeits-Netzen, die Vertrauenswürdigkeit einer Transition und die Informationsvertraulichkeit einer Stelle erläutert. Die Informationsvertraulichkeit einer Stelle wird bestimmt durch die höchste Informationsvertraulichkeitsklasse von allen der Stelle zugewiesenen Informationsobjekten. Eine Zuweisung erfolgt mithilfe einer Anfangsmarkierung (Informationsobjekte sind Marken der Informationsvertraulichkeits-Netze) und den nachfolgenden Schaltvorgängen. Wenn beispielsweise der Objekttyp „Bestellung“ mit der Informationsvertraulichkeitsklasse 1 der Stelle „eingegangene Bestellung“ zugewiesen wird und bisher kein weiteres Objekt der Stelle zugewiesen wurde, ist die Vertraulichkeitsklasse der Stelle demnach 1. Allgemein wird die Informationsvertraulichkeit einer Stelle wie in Definition 5.3 definiert:

Definition 5.3:
Informationsvertraulichkeit einer Stelle
Die ***Informationsvertraulichkeit einer Stelle*** *$C(p,m)$ ist abhängig von der Informationsvertraulichkeit aller Informationsobjekte $C(i)$, welche der Stelle unter der Markierung m zugewiesen sind. Dementsprechend ist $C(p,m)$ definiert:*

$$C(p,m) = \max_{i \in m(p)} C(i)$$

Die Stelle nimmt also die höchste Schutzklasse der enthaltenen Informationsobjekte an, weil davon ausgegangen wird, dass es nicht möglich ist, auf die Stelle zuzugreifen, ohne möglicherweise Kenntnis aller enthaltenen Objekte zu erhalten. Wenn man sich

dieser Annahme nicht anschließen möchte, so kann man die dann entstehenden Netze auf obige Netze transformieren, indem man den Zugriffsautomatismus auf die Stelle (dieser muss dann ja eine hohe Vertrauenswürdigkeit besitzen) als eigene Transition abbildet und so die Marken herausgreift, dann in eine weitere Stelle verschiebt und somit den Zugriff durch die eigentliche Transition ermöglicht. Der vorgeschlagene Ansatz bleibt folglich weiterhin anwendbar.

Die Vertrauenswürdigkeit einer Transition ist definiert als die minimale Vertrauenswürdigkeitsklasse aller der Transition zugewiesenen Ressourcen. Ressourcen können statisch den Transitionen eines Geschäftsprozessmodells oder dynamisch während der simulierten Ausführung eines Geschäftsprozesses zugewiesen werden (Schuster, 2012). Die unterschiedlichen Zuweisungsstrategien können auch kombiniert werden. Wenn beispielsweise dynamisch eine Person „Service-Mitarbeiter" mit einer Vertrauenswürdigkeit von 2 und statisch eine Maschine „Bestellsystem" mit einer Vertrauenswürdigkeit von 1 einer Transition „Kunden informieren" zugewiesen sind, so hat die Transition eine Vertrauenswürdigkeit von 1 (als Minimum der Vertrauenswürdigkeiten aller zugewiesenen Ressourcen). In der vorliegenden Arbeit wird nur die statische Zuweisung weiterverfolgt, weil für die dynamische Zuweisung andere Arbeiten wie beispielsweise Schuster (Schuster, 2012) existieren. Allgemein wird die Vertrauenswürdigkeit einer Transition wie folgt definiert:

Definition 5.4:
Vertrauenswürdigkeit einer Transition
*Die **Vertrauenswürdigkeit einer Transition** $TW(t)$ ist abhängig von der Vertrauenswürdigkeit aller Ressourcen $TW(r)$, die der Transition zugewiesen sind.*
$TW(t)$ ist definiert als:

$$TW(t) = \min_{r \in \{r \mid (r,t) \in RT\}} TW(r)$$

Ablauf-Informationsvertraulichkeit

Die Informationsvertraulichkeit im Ablauf (Ausführung oder Simulation) eines Geschäftsprozesses ist gewährleistet, wenn keine unautorisierte Kenntnisnahme oder Weitergabe von Informationen während der Ausführung des Geschäftsprozesses erfolgt. Dazu muss für jede Transition in einem Geschäftsprozess immer gelten: Transitionen dürfen nur Marken (das heißt Informationsobjekte) von Eingangsstellen konsumieren, die eine Informationsvertraulichkeit C(p, m) besitzen, welche kleiner oder gleich der eigenen Vertrauenswürdigkeit ist (siehe Definition 5.5). Dadurch wird verhindert, dass vertrauliche Informationen von nicht hinreichend vertrauenswürdigen Transitionen (beziehungsweise von nicht hinreichend vertrauenswürdigen Ressourcen, die der Transition zugewiesen sind) verarbeitet werden.

Darüber hinaus dürfen Transitionen nur Marken (das heißt Informationsobjekte) produzieren, die einen Vertraulichkeitswert haben, welcher kleiner oder gleich dem eigenen Vertrauenswürdigkeitswert ist. Dies bedeutet auch, dass es möglich ist, dass eine Transition Informationsobjekte produziert, deren Vertraulichkeit kleiner der eigenen Vertrauenswürdigkeitsklasse ist. Dies verletzt die „No-write-down-Regel“ von Bell & LaPadula (Bell & LaPadula, 1976). Die Regel verhindert, dass jemand unbewusst oder bewusst vertrauliche Informationen deklassifiziert und so Dritten zugänglich macht. Jedoch stehen anders als bei Bell & LaPadula (Bell & LaPadula, 1976) in der vorliegenden Arbeit strukturierte Prozesse zur Verfügung, sodass aufgrund des Prozesses kontrolliert wird, wann ein „Write down“ erfolgt (beispielsweise weil bestimmte Informationen aus einem Informationsobjekt entfernt wurden), und welche Informationstypen mit einer niedrigeren Vertraulichkeitsklasse geschrieben werden. Deswegen wird ein „Write down“ bewusst zugelassen.

Anders sieht es mit dem „Write up“ aus. Bell & LaPadula (Bell & LaPadula, 1976) lassen dies mit dem Argument zu, dass der Schutz der Information nur dadurch verbessert wird, indem man den Zugriff einschränkt. Hier wird dies bewusst nicht ermöglicht, weil man so erreicht, dass diese Klassifizierung nur durch vertrauens-

würdige Ressourcen (dies können auch IT-Systeme sein) vorgenommen wird. Dahinter steht die Überlegung, dass es notwendig ist, eine Vertrauenswürdigkeitsklasse zu besitzen, um vertrauenswürdig entscheiden zu können, ob die Information nur für diese Vertraulichkeitsklasse gilt oder auch für niedrigere Klassen bereitstehen soll. Deswegen wird ein „Write up“ nicht gestattet. Biba (Biba, 1977) gestattet ebenfalls kein „Write up“ mit dem Ziel, die Integrität der Informationen zu fördern. Wenn in weiteren Arbeiten das Schutzziel Integrität in den Ansatz einbezogen werden soll, ist das Vorhandensein des Prinzips bereits ein möglicher Anknüpfungspunkt.

Die Informationsvertraulichkeit der Stelle im Nachbereich der Transition, welche die erzeugte Marke aufnimmt, bestimmt die Vertraulichkeit der produzierten Marke. Wenn die Informationsvertraulichkeit der Ausgangsstelle nicht bestimmt ist, kann die Transition die Informationsvertraulichkeit der produzierten Marke selbst bestimmen und dadurch die Informationsvertraulichkeit der aufnehmenden Ausgangsstelle dynamisch festlegen. Eine Transition kann wie schon erörtert eine Marke produzieren, die eine geringere Informationsvertraulichkeit besitzt als die eingehende Marke. Dies ist nützlich, wenn beispielsweise der Informationsgehalt eines Informationsobjektes durch die Transition reduziert wurde (zum Beispiel, wenn nur noch vier statt alle Stellen einer Kreditkartennummer weiterverarbeitet werden). Dies kann – als Erweiterung der Schaltregel – als Definition 5.5 formalisiert werden.

Ein großer Vorteil der Integration der Informationsvertraulichkeit in Petri-Netze ist, dass vorhandene Analyseverfahren weiter genutzt beziehungsweise auf die Eigenschaften von Informationssicherheits-Netzen angewandt werden können. Dies soll an einem Beispiel verdeutlicht werden. Die genauen Verfahren sind im nachfolgenden Kapitel beschrieben.

Definition 5.5:
klassenbasierte Ablauf-Informationsvertraulichkeit
Wenn $C(p,m)$ die Informationsvertraulichkeit einer Stelle $p \in P$ unter einer Markierung $m \in M$ und $TW(t)$ die Vertrauenswürdigkeit einer Transition $t \in T$ ist, dann können die Bedingungen der Schaltregel für eine aktivierte Transition t erweitert werden und es ergibt sich folgende Schaltregel:

- *In einem klassenbasierten Informationsvertraulichkeits-Netz $cICN = (P,T,F,R,I,IT,RT,ITP,C,CT,TW)$ ist eine Transition $t \in T$ genau dann unter einer Markierung $m: P \to \mathcal{P}(I)$ aktiviert, wenn*

  $\forall p \in \bullet t$: $m(p) \neq \emptyset$,

  $\forall p \in \bullet t$: $C(p,m) \leq TW(t)$ *und*

  $\forall p \in t\bullet$: $\forall it \in t\bullet$: $C(it) \leq TW(t)$.
- *Eine aktivierte Transition kann schalten.*

- *Wenn eine Transition $t \in T$ schaltet, wird die Markierung m in die Markierung m' überführt. m' lässt sich wie folgt ableiten:*

o $\forall p \notin \bullet t \cup t\bullet : m'(p) = m(p)$

o *und* $\forall p \in \bullet t : m'(p) = m(p) \backslash \{i_{konsumiert}\}$ *(wobei für verschiedene Stellen p im Vorbereich der Transition verschiedene $i_{konsumiert}$ von der Transition konsumiert werden können). Für $i_{konsumiert}$ muss gelten $i_{konsumiert} \in m(p)$.*

o *und* $\forall p \in t\bullet : m'(p))m(p) \cup \{i_{produziert}\}$ *(wobei für verschiedene Stellen p im Nachbereich verschiedene $i_{produziert}$ von der Transition produziert werden können).*

Dabei gilt weiterhin:

- $\forall i_{produziert}: C(i) \leq TW(t)$
- *Für eine Stelle p im Nachbereich der Transition und für das für diese Stelle produzierte* $i_{produziert}$ *gilt, falls* $ITP(p) \neq \emptyset$: $C(i_{produziert}) = CT(it), it = ITP(p)$
  Sonst im Standardfall, wenn durch Transition und Nachbereich nicht anders definiert (beispielsweise weil Informationen zum Informationsobjekt i hinzugefügt oder entfernt werden und dadurch vom Standardfall abgewichen wird):
  $C(i_{produziert}) = C(i_{konsumiert})$

Beispiel

Abbildung 11 zeigt ein klassenbasiertes Informationsvertraulichkeits-Netz, welches den Geschäftsprozess einer Bestellabwicklung darstellt. Jeder Transition ist im Beispiel mindestens eine Ressource zugeordnet; die Vertrauenswürdigkeit der jeweiligen Ressource ist in Klammern angegeben. Die Transition „informiere Kunde“ benötigt zur Ausführung zwei Ressourcen: die Maschine „Bestellsystem“ mit der Vertrauenswürdigkeit 1 und die personelle Ressource „Mitarbeiter Kundenhotline“ mit der Vertrauenswürdigkeit 2. Gemäß Definition 5.4 beträgt die Vertrauenswürdigkeit der Transition „informiere Kunde“ Wert 1. Für die meisten Stellen sind Informationsobjekttypen verknüpft und unter der jeweiligen Stelle angegeben. In Klammern ist jeweils die Informationsvertraulichkeit der Informationsobjekttypen benannt. Im Beispiel sind für einige Stellen die Informationsobjekttypen nicht statisch definiert; eine solche Stelle ist beispielsweise „abgelehnte Bestellung“. Das bedeutet nicht, dass Informationsobjekte in der Stelle überhaupt nicht vertraulich sind. Es bedeutet, dass die Informationsvertraulichkeit nicht für alle möglichen Prozessinstanzen vorher statisch bestimmt werden kann. Die Informationsvertraulichkeit ist abhängig von der Transition, die ein Informationsobjekt in der Stelle ablegt, und der spezifischen Prozessinstanz. Abhängig von der dynamisch zugewiesenen Informationsvertraulichkeit

kann dann die nachfolgende Transition schalten oder nicht. Im Falle der Stelle „abgelehnte Bestellung“ kann die nachfolgende Transition „informiere Kunde“ nur schalten, wenn die dynamisch zugewiesene Informationsvertraulichkeit maximal 1 beträgt. Da das Informationsobjekt von der Transition „zurückweisen“ oder von der Transition „nicht erfolgreiche Zahlung“ erzeugt wird, kann seine Informationsvertraulichkeit maximal 3 betragen.

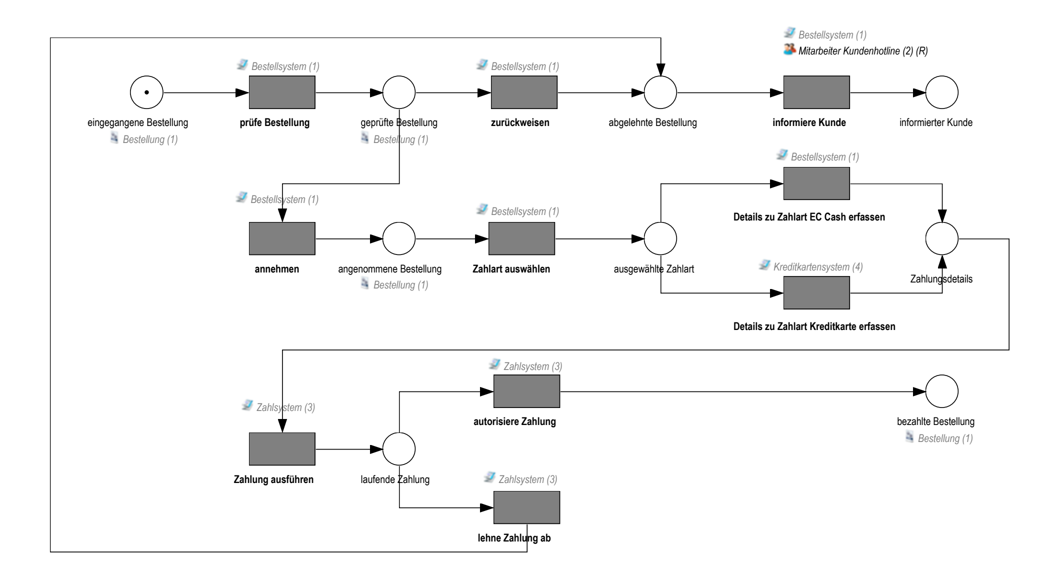


Abbildung 11: Informationsvertraulichkeits-Netz zur Darstellung einer Bestellabwicklung

Die Analyse der Restriktionen in Informationsvertraulichkeits-Netzen kann auf vorhandene Verfahren zurückgeführt werden. Beispielsweise kann die Erreichbarkeitsanalyse genutzt werden, um zu bestimmen, ob eine bestimmte Markierung des Petri-Netzes – ausgehend von einer Startmarkierung – erreicht werden kann oder nicht.

Tabelle 4: Beispielschaltfolge 1

schaltende Transition	Nach dem Schalten Informationsobjekt i in Stelle	C(i)
-	eingegangene Bestellung	1
prüfe Bestellung	geprüfte Bestellung	1
annehmen	angenommene Bestellung	1
Zahlart auswählen	ausgewählte Zahlart	1
Details zu Zahlart Kreditkarte erfassen	Zahlungsdetails	3
Zahlung ausführen	Zahlstatus	2
lehne Zahlung ab	abgelehnte Bestellung	2
Blockierung, weil die Marke über eine zu hohe Informationsvertraulichkeit verfügt, um von der nächsten Transition verarbeitet zu werden.		

Tabelle 5: Beispielschaltfolge 2

schaltende Transition	Nach dem Schalten Informationsobjekt i in Stelle	C(i)
-	eingegangene Bestellung	1
prüfe Bestellung	geprüfte Bestellung	1
annehmen	angenommene Bestellung	1
Zahlart auswählen	ausgewählte Zahlart	1
Details zu Zahlart Kreditkarte erfassen	Zahlungsdetails	3
Zahlung ausführen	Zahlstatus	2
lehne Zahlung ab	abgelehnte Bestellung	1
informiere Kunden	informierter Kunde	0

Im Beispiel wird entsprechend die folgende Fragestellung untersucht: Ist eine Schlussmarkierung (eine Marke in „informierter Kunde“ oder eine Marke in „bezahlte Bestellung“) unter einer gegebenen Anfangsmarkierung erreichbar? Tabelle 4 und Tabelle 5 zeigen zwei verschiedene Schaltfolgen für den dargestellten Geschäftsprozess der Bestellabwicklung. In der Beispielschaltfolge 1 wird eine Blockierung erkannt, die durch das Objekt mit der Informationsvertraulichkeit 2 in der Stelle „abgelehnte Bestellung“ entsteht. Die nachfolgende Transition kann nicht schalten, und es kann keine Schlussmarkierung erreicht werden, das heißt, der Geschäftsprozess kann nicht abgeschlossen werden. Die Restriktion ist sinnvoll, weil die Ressource „Bestellsystem“ nicht auf Informationen über bestimmte, nicht erfolgreiche Zahlvorgänge zugreifen soll (zum Beispiel bei Missbrauch von Kreditkarten).

5.1.2 Rollenbasierte Informationsvertraulichkeit

Mithilfe der gerade vorgestellten klassenbasierten Informationsvertraulichkeit lassen sich bereits einige typische Anforderungen an die Informationsvertraulichkeit gerade in kleineren Organisationen umsetzen. Allerdings lassen sich die beispielhaften Anforderungen „Kenntnisnahme nur für Mitarbeiter der Fachabteilung Bestellabwicklung“ oder „Kenntnisnahme nur durch Mitarbeiter des Projektes Bestellprozessverbesserung“ damit nicht abbilden. Hierfür genügt es nicht, der Ressource nur das Attribut Vertrauenswürdigkeit zuzuordnen; im ersten Fall wäre eine Zuordnung zur Fachabteilung, im zweiten Fall eine (zusätzliche) Zuordnung zur Projektgruppe erforderlich. Außerdem müssten auch die Informationsobjekte diese Beschränkung in geeigneter Weise kennen. Um diese Anforderung abbilden zu können, wird zusätzlich ein rollenbasiertes Verfahren verwendet. Die rollenbasierte Zugriffskontrolle wurde von Ferraiolo & Kuhn (Ferraiolo & Kuhn, 1992) entwickelt und wird inzwischen vielfältig eingesetzt.

Um dies mit Informationsvertraulichkeits-Netzen modellieren zu können, wird das klassenbasierte Informationsvertraulichkeits-Netz cICN wie folgt ergänzt (siehe Definition 5.6):

Definition 5.6:
Informationsvertraulichkeits-Netz
Ein ***Informationsvertraulichkeits-Netz*** *ist ein Tupel* $ICN = (P, T, F, R, I, IT, RT, ITP, C, CT, TW, RO, ROO, ROOT, ROR)$ *mit*

- P *als eine endliche Menge von Stellen,*
- T *als eine endliche Menge von Transitionen,*
- $P \cap T = \emptyset$*,*
- $F \subseteq (P \times T) \cup (T \times P)$ *als eine Flussrelation,*
- R *als eine endliche Menge von Ressourcen,*
- I *als eine Menge von Informationsobjekten,*
- IT *als eine Menge von Informationsobjekttypen,*
- $RT \subseteq (\mathcal{P}(R) \times T)$ *als eine Allokation von Ressourcen zu Transitionen,*
- $ITP \subseteq (\{IT \cup \emptyset\} \times P)$ *als eine Allokation von jeweils keinem oder einem Informationsobjekttypen zu einer Stelle,*
- $C: I \rightarrow \mathbb{N}$ *als die Informationsvertraulichkeit der Information,*
- $CT: IT \rightarrow \mathbb{N}$ *als die Informationsvertraulichkeit des Informationsobjekttyps,*
- $TW: R \rightarrow \mathbb{N}$ *als die Vertrauenswürdigkeit einer Ressource* r*,*
- RO *als eine endliche Menge von Rollen,*
- $ROO: I \rightarrow \mathcal{P}(\mathcal{P}(RO))$ *als die Menge der Mengen der zugriffsberechtigten Rollen zur Information,*
- $ROOT: IT \rightarrow \mathcal{P}(\mathcal{P}(RO))$ *als die Menge der Mengen der zugriffsberechtigten Rollen zum Informationsobjekttyp und*
- $ROR: R \rightarrow \mathcal{P}(RO)$ *als die Menge der Mengen der Rollen, welche als Berechtigung der Ressource zugeordnet sind.*

Hinzu kommen eine endliche Menge an Rollen (RO) sowie die Funktionen $ROO(i)$ und $ROR(r)$. Die Funktion $ROO(i)$ weist einem i eine Menge von Mengen $\{a_1, a_2, \cdots, a_n\}$ zu. Jedes Element a_i ist selbst wieder eine Menge, genauer gesagt eine Teilmenge aller Rollen ($a_i \subseteq RO$). Die Funktion $ROO(i)$ bildet somit eine Information i auf ein Mengensystem (Nef, 1977, S. 10) ab. $ROO(i)$ beschreibt, welche Rolle(n) notwendig sind, um eine Information i zu lesen oder zu verarbeiten. Rollen können mit

einem logischen ‚und' verknüpft sein. Dann sind alle so verknüpften Rollen notwendig, um auf eine Information zuzugreifen. Beispielsweise sollen für den Zugriff auf die Information „Abwicklungsdauer" die Rolle „Fachbereich Bestellwesen" und die Rolle „Projektgruppe Bestellprozessverbesserung" benötigt werden. Diese Anforderung wird dann als eine Menge mit zwei Elementen abgebildet.

Zusätzlich können Rollenanforderungen mit einem nicht exklusiven ‚oder' verknüpft sein. Beispielsweise soll es auch genügen, die Rolle „Geschäftsführer" zu haben. Diese wird dann als einzelne Menge mit einem Element in die Gesamtmenge aufgenommen. So ergibt sich für ROO (Abwicklungsdauer)={{Fachbereich Bestellwesen, Projektgruppe Bestellprozessverbesserung},{Geschäftsführer}}.

Die Funktion $ROR(r)$ liefert zu einer Ressource r eine Menge mit allen Rollen der Ressource zurück. Beispielsweise ist die Ressource „Adam" mit den Rollen „Fachbereich Bestellwesen" und „Projektgruppe Bestellprozessverbesserung" und die Ressource „Eva" mit den Rollen „Controlling", „Forderungsmanagement" und „Ersthelfer" verknüpft. Dementsprechend ist ROR(Adam)={Fachbereich Bestellwesen, Projektgruppe Bestellprozessverbesserung} und ROR(Eva)={Fachbereich Controlling, Forderungsmanagement, Ersthelfer}.

Nun ist die Menge der notwendigen Rollen zum Zugriff auf eine Stelle zu definieren. Dabei wird wieder davon ausgegangen, dass es weiterhin nicht möglich ist, auf die Stelle zuzugreifen, ohne möglicherweise Kenntnis aller enthaltenen Objekte zu erhalten. Enthält eine Stelle ausschließlich das Informationsobjekt x und ist $\mathrm{ROO(x)} = \{\{a\},\{b\}\}$, so soll eine Transition t darauf zugreifen dürfen, wenn allen ihren zugeordneten Ressourcen auch mindestens jeweils die Rolle a oder die Rolle b zugeordnet sind.

Enthält die gleiche Stelle nun zusätzlich zu x das Informationsobjekt y und ist $\mathrm{ROO(y)} = \{\{b\},\{c\}\}$, so soll eine Transition t auf die Stelle zugreifen dürfen, wenn jede ihrer zugeordneten Ressourcen mindestens eine der Rollenmengen $\{b\}$ oder $\{a,c\}$ als

Teilmenge ihrer Rollenmenge besitzt[3]. Also wenn für jedes r $\in \{\mathrm{r}|(\mathrm{r},\mathrm{t}) \in \mathrm{RT}\}$ gilt, dass $(\{ b\} \cap \mathrm{ROR(r)}) \neq \emptyset \vee (\{ a,c\} \cap \mathrm{ROR(r)}) \neq \emptyset$. Die Transition t könnte also beispielsweise schalten, wenn ihr ausschließlich eine Ressource u mit der einzigen Rolle b zugewiesen ist. Die Transition kann aber nicht schalten, wenn ihr zusätzlich eine Ressource v mit der einzigen Rolle c zugewiesen ist. Der Ressource v müsste beispielsweise zusätzlich die Rolle a zugewiesen sein.

Für eine Stelle ist somit zunächst zu klären, welche Rollenmengen den Zugriff erlauben. Dazu wird die folgende ungeordnete Verknüpfung von Mengen definiert.

Definition 5.7:
Verknüpfung von Mengensystemen
*Seien $A_1, A_2, \dots, A_n$ Mengensysteme (Mengen, deren Elemente selbst wieder Mengen sind.), so ist die **Verknüpfung** ⊠ dieser **Mengensysteme**:*

$\boxtimes A_{i=1}^{n}$

$:= A_1 \boxtimes A_2 \boxtimes \cdots \boxtimes A_n$

$:= \{a_1 \cup a_2 \cup \cdots \cup a_n \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n \}$

Die minimale Verknüpfung dieser Mengensysteme ist:

$\boxtimes' A_{i=1}^{n} := \{x | x \in \boxtimes A_{i=1}^{n} \wedge \nexists y \in \boxtimes A_{i=1}^{n}, y \subset x\}$

Die Definition 5.7 wird an einem kurzen Beispiel verdeutlicht. Dazu ist $A_1 = \{\{a\},\{b\},\{c,d\}\}$, $A_2 = \{\{a\},\{c\},\{e\}\}$, und $A_3 = \{\{a\},\{f\}\}$. Dann ist die Verknüpfung $\boxtimes A_{i=1}^{3}$=$\{${a}, {a, c}, {a,e}, $\{a,f\}$,{a,c},{a,c,f}, {a,c,f} ,{a,e,f}, {b,c,f}, {b,e,f} , {c,d,f},{c,d,e,f}$\}$. Die gekürzte Verknüpfung ist dann $\boxtimes' A_{i=1}^{3}$=$\{${a}, {b,c,f}, {b,e,f} ,{c,d,f}$\}$.

[3] {a} oder {c} alleine genügen nicht, da mit nur {a} kein Zugriff auf y erlaubt wäre und mit nur {c} kein Zugriff auf x.

Damit lässt sich die Menge der zulässigen Mengenkombinationen zum Zugriff auf eine Stelle wie folgt definieren:

Definition 5.8:
Rollenmengensystem mit Zugriff auf eine Stelle
*Das **Rollenmengensystem**, das den **Zugriff auf eine Stelle** erlaubt $ROP(p,m)$, ist abhängig von der Menge der zugriffsberechtigten Rollen zur Information i $ROO(i)$, welche der Stelle unter der Markierung m zugewiesen sind. Dementsprechend ist $ROP(p,m)$ definiert:*

$$ROP\ (p,m) = \boxtimes' ROO(i)_{\ i \in m(p)}$$

In Definition 5.8 könnte statt der minimalen auch die ungekürzte Verknüpfung verwendet werden. Die minimale Verknüpfung ist jedoch für menschliche Betrachter besser zu lesen und hat die gleiche Konsequenz, da nicht auch das Vorhandensein einer zugehörigen Obermenge geprüft werden muss, wenn bereits eine Teilmenge zum Zugriff genügt. Definition 5.5 kann mit den rollenbasierten Regeln zu Definition 5.9 erweitert werden:

Definition 5.9:
Ablauf-Informationsvertraulichkeit
Wenn $C(p,m)$ die Informationsvertraulichkeit einer Stelle $p \in P$ unter einer Markierung $m \in M$ und $TW(t)$ die Vertrauenswürdigkeit einer Transition $t \in T$ sind, dann können die Bedingungen der Schaltregel für eine aktivierte Transition t erweitert werden, und es ergibt sich folgende Schaltregel:

- *In einem Informationsvertraulichkeits-Netz $ICN = (P, T, F, R, I, IT, RT, ITP, C, CT, TW, RO, ROO, ROOT, ROR)$ ist eine Transition $t \in T$ genau dann unter einer Markierung $m: P \to \mathcal{P}(I)$ aktiviert, wenn*
  $\forall p \in \bullet t \quad m(p) \neq \emptyset$,
  $\forall p \in \bullet t: \quad C(p,m) \leq TW(t)$,
  $\forall p \in t\bullet: \ \forall it \in t\bullet: \ C(it) \leq TW(t)$ *und*
  $\forall p \in \bullet t \ \wedge \ \forall r \in \{r | (r,t) \in RT\}: \exists\, a_i \in ROP(p,m): a_i \subseteq ROR(r)$ *(a_i ist eine Menge)*

- *Eine aktivierte Transition kann schalten.*

- *Wenn eine Transition $t \in T$ schaltet, wird die Markierung m in die Markierung m' überführt. m' lässt sich wie folgt ableiten:*
  - $\forall p \notin \bullet t \cup t\bullet: \ m'(p) = m(p)$
  - *und* $\forall p \in \bullet t: m'(p) = m(p) \setminus \{i_{konsumiert}\}$ *(wobei für verschiedene Stellen p im Vorbereich der Transition verschiedene $i_{konsumiert}$ von der Transition konsumiert werden können). Für $i_{konsumiert}$ muss gelten $i_{konsumiert} \in m(p)$.*
  - *und* $\forall p \in t\bullet: m'(p) = m(p) \cup \{i_{produziert}\}$ *(wobei für verschiedene Stellen p im Nachbereich verschiedene $i_{produziert}$ von der Transition produziert werden können).*

Dabei gilt weiterhin:

- $\forall i_{produziert}: C(i) \leq TW(t)$
- *Für eine Stelle p im Nachbereich der Transition und für das für diese Stelle produzierte $i_{produziert}$ gilt, falls $ITP(p) \neq \emptyset$: $C(i_{produziert}) = CT(it), it = ITP(p) \wedge ROO(i_{produziert}) = ROOT(it)$*
  Sonst im Standardfall, wenn durch Transition und Nachbereich nicht anders definiert (beispielsweise weil Informationen zum Informationsobjekt i hinzugefügt oder entfernt werden und dadurch vom Standardfall abgewichen wird):
  $C(i_{produziert}) = C(i_{konsumiert}) \wedge ROO(i_{produziert}) = ROO(i_{konsumiert})$

Die neue Bedingung $\forall p \in {}^{\bullet}t \wedge \forall r \in \{r|(r,t) \in RT\}: \exists a_i \in ROP(p,m): a_i \subseteq ROR(r)$ drückt die neue Forderung aus. Für jede Stelle p im Vorbereich der Transition muss für jede Ressource r der Transition gelten, dass sie ein Element innerhalb der Menge ROP(p, m) besitzt, welches eine Teilmenge von ROR(r) ist. Dadurch wird sichergestellt, dass die Ressource eine berechtigende Rollenkombination besitzt. Verletzt nur eine zugewiesene Ressource diese Bedingung, darf die Transaktion nicht auf das Element zugreifen und somit nicht schalten. Zudem wurde die Schaltregel erweitert, um zu definieren, welche Rollenkombination Zugriff auf das neue Informationsobjekt $i_{produziert}$ haben soll.

5.2 Datenschutz

Im vorangegangenen Teilkapitel Informationsvertraulichkeit wurden alle Informationen unabhängig von ihrer Art betrachtet. So wurde beispielsweise auch der Schutz von Geschäfts- beziehungsweise Betriebsgeheimnissen (zum Beispiel geheimes Produktionsrezept/-verfahren) ermöglicht. Im nun folgenden Teilkapitel ist hingegen „nur“ der Datenschutz von Interesse, im Fokus stehen also Informationen, welche Aussagen zu natürlichen Personen treffen.

Grundsätzlich gibt es vor und während der Verarbeitung von personenbezogenen Daten gesetzliche Rahmenbedingungen zu beachten. Abbildung 12 gibt einen vereinfachten Überblick dazu.

Im Datenschutz gilt das Prinzip „Verbot mit Erlaubnisvorbehalt“. Da die Verarbeitung personenbezogener Daten aufgrund des Datenschutzrechtes grundsätzlich verboten ist[4], muss, wenn es einen Anlass zur Verarbeitung personenbezogener Daten gibt, geprüft werden, ob ein Erlaubnistatbestand vorliegt, welcher die beabsichtigte Datenverarbeitung erlaubt. Die EU-Datenschutz-Grundverordnung listet in Artikel 6 die Erlaubnistatbestände auf. Ein solcher Erlaubnistatbestand kann beispielsweise aufgrund eines Gesetzes bestehen. Die Einwilligung ist, abgesehen vom öffentlichen Bereich der staatlichen Datenverarbeitung, der „wichtigste“ Erlaubnistatbestand (Körner, 2000, S. 141). Die praktische Bedeutung der Einwilligung hat seitdem nicht abgenommen, somit ist die Einwilligung nach Inkrafttreten der neuen europäischen Datenschutz-Grundverordnung der „zentrale“ Erlaubnistatbestand (Buchner & Kühling, 2017, S. 544). Der Gesetzgeber hat einige Bedingungen – wie beispielsweise die Informiertheit – an eine wirksame Einwilligung aufgestellt.

Die Verarbeitung personenbezogener Daten aus besonderen Kategorien (zum Beispiel ethnische Herkunft, religiöse oder weltanschauliche Überzeugung, genetische Daten) ist nach Artikel 9 Absatz 1 verboten. Absatz 2 regelt hier gesondert die Erlaubnistatbestände. Auch für Daten dieser Kategorie ist die Einwilligung des Betroffenen als Erlaubnistatbestand geregelt.

Liegt eine Legitimation vor, kann die Datenerhebung erfolgen. Die erhobenen Daten können danach verarbeitet werden, solange die Legitimation nicht beispielsweise durch Widerruf der Einwilligung weggefallen ist.

---

[4] Dieses Verbot ist insbesondere immer dann gegeben, wenn der sachliche Anwendungsbereich der EU-DS-GVO eröffnet ist. Eine Ausnahme davon ist beispielsweise die Verarbeitung von personenbezogenen Daten „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ (Artikel 2, Absatz 2, lit. c, EU-DS-GVO). Weitere Überlegungen zur Anwendbarkeit der EU-DS-GVO finden sich beispielsweise bei Kieck & Pohl (Kieck & Pohl, 2017).

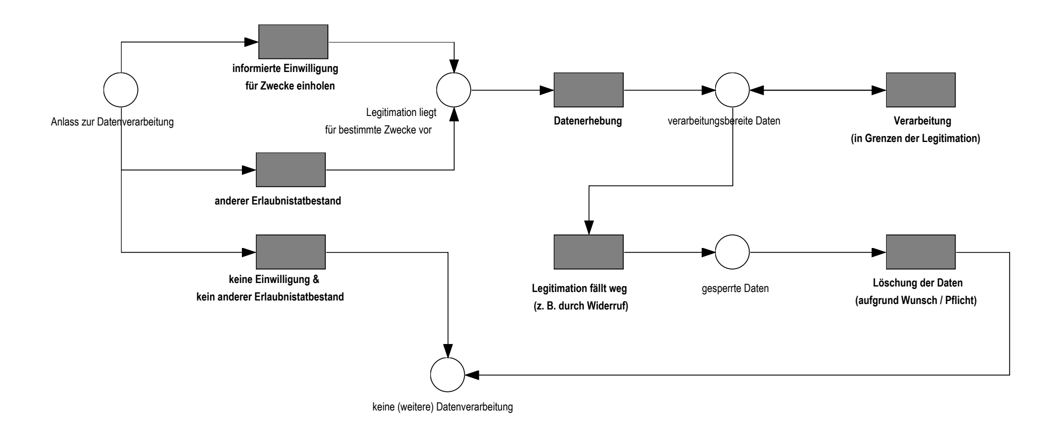


Abbildung 12: vereinfachte Darstellung ausgewählter Rahmenbedingungen an die Verarbeitung personenbezogener Daten

Danach dürfen die Daten nicht weiterverarbeitet werden und sind ggf. auch zu löschen. Ist von Beginn an kein Erlaubnistatbestand erfüllt, darf keine Datenverarbeitung erfolgen.

5.2.1 Zweckbindung

Die Zweckbindung ist einer der von der europäischen Datenschutz-Grundverordnung geforderten Grundsätze (Artikel 5, Absatz 1, lit. b). Personenbezogene Daten dürfen also nur für zuvor legitimierte Zwecke erhoben und zu diesen verarbeitet werden. Der erlaubte Zweck beziehungsweise die erlaubten Zwecke ergeben sich aus dem Erlaubnistatbestand – oft also aus der Einwilligungserklärung oder dem Vertrag, für den die Verarbeitung erforderlich ist. Es gibt eine Ausnahme von der Zweckbindung für „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ (Artikel 5, Absatz 1, lit. b) der Daten.

Zur Betrachtung der Zweckbindung innerhalb der Geschäftsprozessmodellierung werden Informationen um die erlaubten Verarbeitungszwecke angereichert.

Definition 5.10:
Zweckbindungs-Netz
*Ein **Zweckbindungs-Netz** ist ein Tupel $PLN = (P, T, F, I, IT, ITP, Z, L, G, LA, LD, LN, PD, CPD)$ mit*

- *P als eine endliche Menge von Stellen,*
- *T als eine endliche Menge von Transitionen,*
- *$P \cap T = \emptyset$,*
- *$F \subseteq (P \times T) \cup (T \times P)$ als eine Flussrelation,*
- *I als eine Menge von Informationsobjekten,*
- *IT als eine Menge von Informationsobjekttypen,*
- *$ITP \subseteq (\{IT \cup \emptyset\} \times P)$ als eine Allokation von jeweils keinem oder einem Informationsobjekttypen zu einer Stelle,*
- *Z als eine endliche Menge von Zwecken,*
- *$L: I \times M \rightarrow \{\mathcal{P}(Z)\}$ als die Menge der unter einer Markierung mit einer Information verknüpften (das heißt erlaubten) Zwecke,*
- *$G: P \times T \rightarrow \{\mathcal{P}(Z)\}$ als die Menge der mit einer Eingangskante zur Transition t aus der Stelle p im Vorbereich der Transition verbundenen Zwecke,*
- *$LA: P \times T \rightarrow \{\mathcal{P}(Z)\}$ als die Menge der mit einer Ausgangskante der Transition t zur Stelle p im Nachbereich der Transition verbundenen Zwecke zur Ergänzung von L(i), also der Zwecke des produzierten Informationsobjektes,*
- *$LD: P \times T \rightarrow \{\mathcal{P}(Z)\}$ als die Menge der mit einer Ausgangskante der Transition t zur Stelle p im Nachbereich der Transition verbundenen Zwecke zur Reduktion von L(i), also der Zwecke des produzierten Informationsobjektes,*
- *$LN: P \times T \rightarrow \{\mathcal{P}(Z)\}$ als die Menge der mit einer Ausgangskante der Transition t zur Stelle p im Nachbereich der Transition verbundenen Zwecke für L(i), also der Zwecke des produzierten Informationsobjektes. Diese Menge ersetzt die bisherige Zwecke-Menge. Daher gilt auch $LN \neq \emptyset \Rightarrow LA = \emptyset \wedge LD = \emptyset$,*
- *$PD: I \rightarrow \{true, false\}$ als eine Funktion, die angibt, ob es sich bei der Information i um ein personenbezogenes Datum handelt oder nicht, und*
- *$CPD: T \times P \rightarrow \{\emptyset, true, false\}$, das angibt, ob ein produziertes Informationsobjekt personenbezogene Daten enthält (true) oder keine personenbezogenen Daten enthält (false).*

Anders als bei der Vertrauenswürdigkeit beim Informationsvertraulichkeits-Netz werden die Zwecke beim Zweckbindungs-Netz nicht mit der Transition, sondern mit den eingehenden Kanten verknüpft. Dies wird je Kante durch G(p, t) beschrieben. Dadurch wird einerseits ermöglicht, je Stelle im Vorbereich einer Transition anzugeben, zu welchen Zwecken die Information von der Transition benötigt wird. Somit kann andererseits auch abgebildet werden, dass eine Transition verschiedene Informationen aus verschiedenen Stellen zu unterschiedlichen Zwecken benötigt. Gleichzeitig soll so verdeutlich werden, dass die damit verknüpfte Bedingung nicht unbedingt von allen Marken (d. h. Informationsobjekten) in einer Stelle des Vorbereichs erfüllt werden muss, sondern ausschließlich von den Marken, die für einen Schaltvorgang von der Transition konsumiert werden. Die formalisierte Schaltregel lautet:

Definition 5.11:
Markierung eines Zweckbindungs-Netzes
*Eine **Markierung** m **eines Zweckbindungs-Netzes** PLN ist eine Funktion $m: P \rightarrow \mathcal{P}(I)$, welche jeder Stelle $p \in P$ Informationsobjekte i zuordnet. Dabei kann einer Stelle unter einer Markierung m kein, ein oder mehrere Informationsobjekt(e) i zugeordnet werden.*
Es gilt weiter: Die Menge M ist die Menge der Markierungen.

Aus Transitionen ausgehende Kanten können durch die Menge LN beschriftet werden. In diesem Fall wird die Zweckbindung des produzierten Informationsobjektes auf die Menge LN gesetzt. Ist keine Menge LN angegeben, kann die Zweckbindung aufgrund der eingehenden Informationsobjekte und der Kantenbeschriftungen LA und LD bestimmt werden. Dann soll die Zweckbindung der eingehenden Information des gleichen Typs übernommen werden und um LA ergänzt beziehungsweise um LD reduziert werden.

Die Zweckbindung eines Informationsobjektes wird zunächst bei der Feststellung des Erlaubnistatbestandes festgelegt, also beispielsweise beim Erteilen der Einwilligung.

Bestimmte Transitionen, die solche Erlaubnistatbestände feststellen, dürfen also erlaubte Zwecke zu einem Informationsobjekt hinzufügen. L(i) bekommt durch diese Transitionen neue Elemente hinzugefügt. Andere Transitionen sind dafür verantwortlich, den Wegfall eines Erlaubnistatbestandes (beispielsweise den Widerruf der Einwilligung) umzusetzen, und entfernen dementsprechend Zwecke aus der Menge L(i). Normale Transitionen haben dagegen keine Auswirkungen auf die Menge L(i), es sei denn, dass sie den Personenbezug aus den Daten entfernen (PD(i) wird dann false).

Zusätzlich kann *„CPD = true“* (das heißt, es handelt sich um ein personenbezogenes Datum) beziehungsweise *„CPD = false“* (das heißt, es handelt sich um kein personenbezogenes Datum) mit ausgehenden Kanten einer Transition verknüpft werden. Dadurch wird das Attribut PD des durch die Transition produzierten Informationsobjektes i auf *true* beziehungsweise *false* gesetzt und somit angegeben, ob das produzierte Informationsobjekt personenbezogene Daten enthält oder nicht. Wenn CPD nicht als Kanteninschrift angegeben, das heißt $CPD = \emptyset$ ist, bleibt diese Eigenschaft wenn möglich unverändert (siehe Schaltregel).

Definition 5.12:
Schaltregel mit Berücksichtigung der Zweckbindung im Ablauf

- *In einem Zweckbindungs-Netz* $PLN = PLN = (P, T, F, I, IT, ITP, Z, L, G, LA, LD, LN, PD, CPD)$ *ist eine Transition* $t \in T$ *genau dann unter einer Markierung* $m: P \to \mathcal{P}(I)$ *aktiviert, wenn für alle* $p \in \bullet t$ *gilt*
  $m(p) \neq \emptyset$ *und*
  $\exists i^*: i^* \in m(p) \wedge (L(i^*) \subseteq G(p,t) \ \vee \ PD(i) = false)$
- *Eine aktivierte Transition kann schalten.*
- *Wenn eine Transition* $t \in T$ *schaltet, wird die Markierung* $m: P \to \mathcal{P}(I)$ *in die Markierung* $m': P \to \mathcal{P}(I)$ *überführt.* m' *lässt sich wie folgt berechnen:*
  $$m' = \begin{cases} m(p) \backslash i^* & falls\ p \in \bullet t\ für\ ein\ i^* \in m(p) \wedge L(i^*) \subseteq G(p,t) \\ m(p) \cup i^\circ & falls\ p \in t \bullet\ für\ und\ falls\ ITP(p) \neq \emptyset\ dann\ Typ(i^\circ) = IPT(p) \\ m(p) & sonst \end{cases}$$
- $L(i^\circ)$ *in m‘ ist für den Nachbereich* $p \in t \bullet$ *der schaltenden Transition t jeweils abhängig von der Beschriftung der Kante (t, p):*
  $$L(i^\circ) = \begin{cases} LN(t,p) & falls\ LN(t,p) \neq \emptyset \\ \big(L(i^*) \backslash LD(t,p)\big) \cup LA(t,p) & falls\ LN(t,p) = \emptyset \wedge \exists i^* | Typ(i^*) = Typ(i^\circ) \\ LD(t,p)) \cup LA(t,p) & sonst \end{cases}$$
- $$PD(i) = \begin{cases} CPD(t,p) & CPD(t,p) \neq \emptyset \\ PD(i^*) & falls\ CPD(t,p) = \emptyset\ \wedge \exists i^* | Typ(i^*) = Typ(i^\circ) \\ false & sonst \end{cases}$$

wobei $Typ: I \to IT$ *zu einem Informationsobjekt i den Informationsobjekttyp it angibt.*

Abbildung 13 veranschaulicht dies an einem Beispiel: Ein Interessent befindet sich auf einer Registrierungswebseite und gibt dort an, ob er den Kontakt entweder per E-Mail oder per Telefon für die Information über ein Produkt erlauben möchte. Je nach Angabe wird entweder der Zweck Werbemail oder Werbeanruf mit den eingegebenen personenbezogenen Daten verbunden. Danach befindet sich dieses Informationsobjekt des Typs „Kundendaten“ in der Stelle „potenzieller Kunde“. In Abhängigkeit der Zweckbindung kann anschließend entweder die Transition „Kunde

per Mail auf neues Produkt hinweisen“ oder die Transition „Kunde mit Produktwerbung kontaktieren“ schalten. Das Resultat ist in beiden Fällen ein informierter potenzieller Kunde.

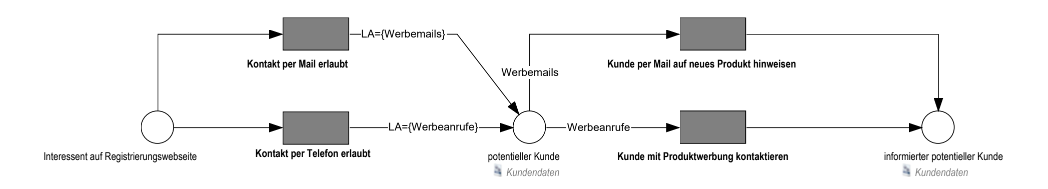


Abbildung 13: Beispiel für ein Zweckbindungs-Netz

5.2.2 Datenminimierung

Der Grundsatz der Datenminimierung (im alten BDSG als Datensparsamkeit bezeichnet) bezieht sich ausschließlich auf personenbezogene Daten (Wagner & Raabe, 2016). Daten, die nicht auf Personen bezogen werden können, müssen folglich nicht betrachtet werden. Um den Grundsatz der Datenminimierung betrachten zu können, werden die Transitionen mit den benötigten Typen von personenbezogenen Daten (wie beispielsweise Vorname, Name, Geburtsdatum) annotiert.

Definition 5.13:
Petri-Netz mit Annotationen zur Analyse der Datenminimierung
Ein Petri-Netz mit Annotationen zur Analyse der Datenminimierung ist ein Tupel $DEN = (P, T, F, D, DT)$ mit

- *P als eine endliche Menge von Stellen,*
- *T als eine endliche Menge von Transitionen,*
- *$P \cap T = \emptyset$,*
- *$F \subseteq (P \times T) \cup (T \times P)$ als eine Flussrelation,*
- *D als die Menge der Typen von personenbezogenen Daten und*
- *$DT: T \rightarrow \mathcal{P}(D)$ als die Menge der für die Ausführung einer Transition benötigten Typen von personenbezogenen Daten.*

Die Annotation ermöglicht es, bei der späteren Analyse der Netze Aussagen zu bestimmten Aspekten der Datenminimierung zu treffen. Dabei ist zu beachten, dass zwar aus der Nichtverwendung auf die Nichterforderlichkeit einer Information geschlossen werden kann, aber dass andererseits die Verwendung nur ein Indiz für die Erforderlichkeit des Informationsobjektes ist. Die verantwortliche Stelle ist angehalten, „Gestaltungsmöglichkeiten der Verarbeitung unter Verzicht auf personenbezogene Daten zu prüfen" (Raabe & Wagner, 2016). Eine Datenverarbeitung ist für einen bestimmten Zweck erforderlich, wenn der Zweck „sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise" (Jandt, 2017) erreicht werden kann. Es ist also zu prüfen, ob es eine andere „datenschutzrechtlich weniger eingreifende Verarbeitungsform […]" gibt (Jandt, 2017). Diese Prüfung ist auf die „konkreten Ausgestaltungsaspekte" zu beziehen (Jandt, 2017), und es muss auch an die Möglichkeit der Anonymisierung und Pseudonymisierung gedacht werden (Raabe & Wagner, 2016). Ein Beispiel ist die Untersuchung einer Blutprobe durch ein Labor im Zuge einer Auftragsverarbeitung. Hier kann, sofern die Abrechnung über den auftraggebenden Arzt erfolgt, die Blutprobe nur zusammen mit einem Pseudonym an das Labor weitergegeben werden. Das Labor muss beispielsweise den Vor- und Nachnamen des

Patienten zur Untersuchung nicht kennen. Es genügt, wenn der Arzt das Pseudonym danach wieder dem Patienten zuordnen kann.

Eine Verarbeitung muss also geeignet und erforderlich (mildestes Mittel) zur Erreichung eines bestimmten Zweckes sein. Zudem muss aber insbesondere im Falle einer Datenschutz-Folgeabschätzung auch die Verhältnismäßigkeit beachtet werden. Dazu muss die Datenverarbeitung beziehungsweise die Schwere ihres Eingriffs in die Persönlichkeitsrechte der Betroffenen in Beziehung zu dem mit ihr verfolgten Zweck gesetzt werden (Jandt, 2017). „Je umfassender und intensiver die Datenverarbeitung ist, desto höherrangiger muss der Zweck einzuordnen sein." (Jandt, 2017)

5.3 Informationsvertraulichkeits- und Datenschutz-Netz

In vielen Anwendungsfällen ist es sinnvoll, neben Datenschutz auch Informationsvertraulichkeit zu betrachten. Dies ergibt sich beispielsweise daraus, dass die Sicherstellung der Informationsvertraulichkeit je nach ihrer Ausprägung beziehungsweise ihrem Zielobjekt eine Maßnahme für den Datenschutz sein kann. Daher wird das Informationsvertraulichkeits-Netz aus Definition 5.6 in Abschnitt 5.1.2 mit dem Zweckbindungs-Netz aus Definition 5.10 in Abschnitt 5.2.1 und dem Netz mit annotierten Datenbedürfnissen aus Definition 5.13 in Abschnitt 5.2.2 kombiniert. Es ergibt sich das Informationsvertraulichkeits- und Datenschutz-Netz.

Definition 5.14:
Informationsvertraulichkeits- und Datenschutz-Netz
Ein Informationsvertraulichkeits- und Datenschutz-Netz ist ein Tupel $ICPN = (P, T, F, R, I, IT, RT, ITP, C, CT, TW, RO, ROO, ROOT, ROR, Z, L, G, LA, LD, LN, PD, CPD, D, DT)$ *mit*

- P *als eine endliche Menge von Stellen,*
- T *als eine endliche Menge von Transitionen,*
- $P \cap T = \emptyset$*,*
- $F \subseteq (P \times T) \cup (T \times P)$ *als eine Flussrelation,*
- R *als eine endliche Menge von Ressourcen,*
- I *als eine Menge von Informationsobjekten,*
- IT *als eine Menge von Informationsobjekttypen,*
- $RT \subseteq (\mathcal{P}(R) \times T)$ *als eine Allokation von Ressourcen zu Transitionen,*
- $ITP \subseteq (\{IT \cup \emptyset\} \times P)$ *als eine Allokation von jeweils keinem oder einem Informationsobjekttypen zu einer Stelle,*
- $C: I \rightarrow \mathbb{N}$ *als die Informationsvertraulichkeit der Information,*
- $CT: IT \rightarrow \mathbb{N}$ *als die Informationsvertraulichkeit des Informationsobjekttyps,*
- $TW: R \rightarrow \mathbb{N}$ *als die Vertrauenswürdigkeit einer Ressource* r*,*
- RO *als eine endliche Menge von Rollen,*
- $ROO: I \rightarrow \mathcal{P}(\mathcal{P}(RO))$ *als die Menge der Mengen der zugriffsberechtigten Rollen zur Information,*
- $ROOT: IT \rightarrow \mathcal{P}(\mathcal{P}(RO))$ *als die Menge der Mengen der zugriffsberechtigten Rollen zum Informationsobjekttyp,*
- $ROR: R \rightarrow \mathcal{P}(RO)$ *als die Menge der Mengen der Rollen, welche als Berechtigung der Ressource zugeordnet sind,*
- Z *als eine endliche Menge von Zwecken,*
- $L: I \times M \rightarrow \{\mathcal{P}(Z)\}$ *als die Menge der unter einer Markierung mit einer Information verknüpften (das heißt erlaubten) Zwecke,*
- $G: P \times T \rightarrow \{\mathcal{P}(Z)\}$ *als die Menge der mit einer Eingangskante zur Transition* t *aus der Stelle* p *im Vorbereich der Transition verbundenen Zwecke,*
- $LA: P \times T \rightarrow \{\mathcal{P}(Z)\}$ *als die Menge der mit einer Ausgangskante der Transition* t *zur Stelle* p *im Nachbereich der Transition verbundenen Zwecke zur Ergänzung von* $L(i)$*, also der Zwecke des produzierten Informationsobjektes,*

- $LD: P \times T \rightarrow \{\mathcal{P}(Z)\}$ *als die Menge der mit einer Ausgangskante der Transition t zur Stelle p im Nachbereich der Transition verbundenen Zwecke zur Reduktion von L(i), also der Zwecke des produzierten Informationsobjektes,*
- $LN: P \times T \rightarrow \{\mathcal{P}(Z)\}$ *als die Menge der mit einer Ausgangskante der Transition t zur Stelle p im Nachbereich der Transition verbundenen Zwecke für L(i), also der Zwecke des produzierten Informationsobjektes. Diese Menge ersetzt die bisherige Zwecke-Menge. Daher gilt auch* $LN \neq \emptyset \Rightarrow LA = \emptyset \wedge LD = \emptyset$*,*
- $PD: I \rightarrow \{true, false\}$ *als eine Funktion, die angibt, ob es sich bei der Information i um ein personenbezogenes Datum handelt oder nicht,*
- $CPD: T \times P \rightarrow \{\emptyset, true, false\}$ *das angibt, ob ein produziertes Informationsobjekt personenbezogene Daten enthält (true) oder keine personenbezogenen Daten enthält (false),*
- D *als die Menge der Typen von personenbezogenen Daten und*
- $DT: T \rightarrow \mathcal{P}(D)$ *als die Menge der für die Ausführung einer Transition benötigten Typen von personenbezogenen Daten.*

Es ergibt sich folgende Definition 5.15 für die Markierung eines solchen Informationsvertraulichkeits- und Datenschutz-Netzes (aufbauend auf Definition 5.11):

Definition 5.15:
Markierung eines Informationsvertraulichkeits- und Datenschutz-Netzes
Eine ***Markierung*** m ***eines Informationsvertraulichkeits- und Datenschutz-Netzes*** $ICPN = (P, T, F, R, I, IT, RT, ITP, C, CT, TW, RO, ROO, ROOT, ROR, Z, L, G, LA, LD, LN, PD, CPD, D, DT)$ *ist eine Funktion* $m: P \rightarrow \mathcal{P}(I)$*, welche unter der Markierung m jeder Stelle* $p \in P$ *Informationsobjekte* $i \in I$ *zuordnet. Dabei können einer Stelle keine Informationsobjekte, ein Informationsobjekt oder auch mehrere Informationsobjekte zugeordnet werden.*
Es gilt weiter: Die Menge M ist die Menge der Markierungen.

Die Schaltregel ergibt sich aus den Schaltregeln aus Definition 5.9 und Definition 5.12. Die neue Schaltregel in Definition 5.16 berücksichtigt sowohl die Informationsvertraulichkeit als auch die Zweckbindung im Ablauf, das bedeutet, dass beide Eigenschaften gleichzeitig gewährleistet werden. Die bekannten Schaltregeln von Petri-Netzen (wie sie in Kapitel 4.3.1 beschrieben sind) werden erweitert, was zu zusätzlichen Schaltbedingungen führt. Das heißt, damit eine Transition aktiviert ist und feuern kann, müssen zusätzliche Bedingungen erfüllt werden. Diese betreffen einerseits die Ablaufvertraulichkeit (die Regeln der klassen- und rollenbasierten Informationsvertraulichkeit müssen eingehalten werden) und die Zweckbindung (Transitionen, die zu einer Verletzung der Zweckbindung führen würden, dürfen nicht schalten). Die produzierten Informationsobjekte (d. h. die Marken) betreffen eine andere Art der Erweiterung und definieren die Informationsvertraulichkeit und die Zweckbindung der Marken.

Definition 5.16:
Schaltregel mit Berücksichtigung der Zweckbindung und Informationsvertraulichkeit im Ablauf
Wenn $C(p,m)$ die Informationsvertraulichkeit einer Stelle $p \in P$ unter einer Markierung $m \in M$ und $TW(t)$ die Vertrauenswürdigkeit einer Transition $t \in T$ sind, dann können die Bedingungen der Schaltregel für eine aktivierte Transition t erweitert werden, und es ergibt sich folgende Schaltregel:

- *In einem Informationsvertraulichkeits- und Datenschutz-Netz $ICPN = (P, T, F, R, I, IT, RT, ITP, C, CT, TW, RO, ROO, ROOT, ROR, Z, L, G, LA, LD, LN, PD, CPD, D, DT)$ ist eine Transition $t \in T$ genau dann unter einer Markierung $m: P \rightarrow \mathcal{P}(I)$ aktiviert, wenn*
  $\forall p \in \bullet t: \quad m(p) \neq \emptyset$,
  $\forall p \in \bullet t: : C(p,m) \leq TW(t)$,
  $\forall p \in \bullet t: \exists i^*: i^* \in m(p) \wedge (L(i^*) \subseteq G(p,t) \vee PD(i) = false)$,
  $\forall p \in t \bullet: \quad \forall it \in t^{\bullet} : C(it) \leq TW(t)$ *und*
  $\forall p \in \bullet t \wedge \forall r \in \{r | (r,t) \in RT\}: \exists a_i \in ROP(p,m): a_i \subseteq ROR(r)$ *(a_i ist eine Menge)*
- *Eine aktivierte Transition kann schalten.*

- *Wenn eine Transition $t \in T$ schaltet, wird die Markierung m in die Markierung m' überführt. m' lässt sich wie folgt ableiten:*

o $\forall p \notin \bullet t \cup t \bullet : m'(p) = m(p)$

o *und* $\forall p \in \bullet t: m'(p) = m(p) \backslash \{i_{konsumiert}\}$ *(wobei für verschiedene Stellen p im Vorbereich der Transition verschiedene $i_{konsumiert}$ von der Transition konsumiert werden können). Für $i_{konsumiert}$ muss gelten $i_{konsumiert} \in m(p) \wedge L(i_{konsumiert}) \subseteq G(p,t)$.*

o *und* $\forall p \in t \bullet : m'(p))m(p) \cup \{i_{produziert}\}$ *(wobei für verschiedene Stellen p im Nachbereich verschiedene $i_{produziert}$ von der Transition produziert werden können). Falls $ITP(p) \neq \emptyset$ dann $Typ(i_{produziert}) = IPT(p)$.*

Es gilt weiterhin:

- $\forall i_{produziert}: C(i) \leq TW(t)$
- *Für eine Stelle p in Nachbereich der Transition und für das für diese Stelle produzierte* $i_{produziert}$ *gilt, falls* $ITP(p) \neq \emptyset$: $C(i_{produziert}) = CT(it), it = ITP(p) \wedge ROO(i_{produziert}) = ROOT(it)$

  Sonst im Standardfall, wenn durch Transition und Nachbereich nicht anders definiert (beispielsweise weil Informationen zum Informationsobjekt i hinzugefügt oder entfernt werden und dadurch vom Standardfall abgewichen wird):

  $C(i_{produziert}) = C(i_{konsumiert}) \wedge ROO(i_{produziert}) = ROO(i_{konsumiert})$
- $L(i°)$ *in m‘ ist für den Nachbereich* $p \in t^{\bullet}$ *der schaltenden Transition t jeweils abhängig von der Beschriftung der Kante (t, p):*

  $$L(i°) = \begin{cases} LN(t,p) & falls\ LN(t,p) \neq \emptyset \\ \left(L(i^*)\backslash LD(t,p)\right) \cup LA(t,p) & falls\ LN(t,p) = \emptyset \wedge \exists i^* | Typ(i^*) = Typ(i°) \\ LD(t,p)) \cup LA(t,p) & sonst \end{cases}$$
- $$PD(i) = \begin{cases} CPD(t,p) & CPD(t,p) \neq \emptyset \\ PD(i^*) & falls\ CPD(t,p) = \emptyset\ \wedge \exists i^* | Typ(i^*) = Typ(i°) \\ false & sonst \end{cases}$$

wobei $Typ: I \rightarrow IT$ *zu einem Informationsobjekt i den Informationsobjekttyp it angibt.*

6 Simulations- und Analyseverfahren für Informationsvertraulichkeits- und Datenschutz-Netze

Informationsvertraulichkeits- und Datenschutz-Netze dienen dazu, Anforderungen der Informationsvertraulichkeit und des Datenschutzes an Geschäftsprozesse und die beteiligten Ressourcen formal zu beschreiben. Die dazu notwendige Formalisierung und Spracherweiterung wurde im vorangehenden Kapitel beschrieben. Dieses Kapitel widmet sich der Frage, welche Auswirkungen die Beachtung der Anforderungen auf die Geschäftsprozesse sowie ihre Ausführung haben. Um zuvor spezifizierte Modelle hinsichtlich ihrer Eigenschaften zu untersuchen, gibt es verschiedene Möglichkeiten. Schuster (Schuster, 2012, S. 14) teilt diese in fünf Kategorien ein: 1) „Diskussion von Modellen (Kreativitätstechniken, etwa die Metaplan-Methode, auch Workshops)“, 2) „Vergleichende Untersuchungen (zum Beispiel Benchmarking, Referenzanalyse, Checklistentechniken)“, 3) „Validierung der Modelle gegenüber festgelegten Metriken“, 4) „Analytische Untersuchung der Modellstruktur“ und 5) „Simulation der Modelle“. In diesem Kapitel werden für Informationsvertraulichkeits- und Datenschutz-Netze vor allem Methoden nach 3), 4) und 5) der obigen Einteilung vorgestellt und dazu auf ihre Teilmenge Informationsvertraulichkeits- und Datenschutz-Netze, welche zusätzlich die Workflow-Bedingungen erfüllen, eingeschränkt. Für Geschäftsprozesse ist diese Einschränkung sinnvoll und eröffnet weitere Analysemöglichkeiten, weil für Workflow-Netze mehr Verfahren zur Verfügung stehen und übertragen werden können.

6.1 Fragestellungen

Folgende Fragestellungen sollen durch die Verfahren betrachtet werden:

1. Wie wirken sich die Anforderungen der Informationsvertraulichkeit und des Datenschutzes auf die Geschäftsprozesse aus, das heißt beispielsweise auf deren Ausführbarkeit?
2. Welche Vertrauenswürdigkeit müssen Ressourcen mindestens besitzen, um wie vorgesehen an einem bestimmten Prozess mitzuwirken? Im Fall der rollenbasierten Informationsvertraulichkeit ist die minimale Rollenkombination gesucht. Dies muss jedoch nicht die Menge mit der kleinsten Anzahl an Elementen sein. Gesucht ist vielmehr die „unkritischste" Menge, bezogen auf die weiteren Möglichkeiten im Hinblick auf die Rollen.
3. Welche Daten werden im Rahmen der Ausführung eines Prozesses verarbeitet (Indikator für Datenminimierung)?
4. Sofern es zur Erreichung eines Ziels mehrere Alternativen gibt (mehrere Modelle oder ein Modell mit alternativen Pfaden): Welches ist der datensparsamste Weg (Pfad)?
5. Für welche Zwecke wird ein Datum verarbeitet?

6.2 Simulation

Nach Hedtstück (Hedtstück, 2013, S. 16) ist unter Simulation die experimentelle Untersuchung eines Modells „mit dem Ziel, neue Erkenntnisse über das System zu gewinnen und daraus Handlungsanweisungen abzuleiten" zu verstehen. Experimentell bedeutet bei der Simulation von Geschäftsprozessen mithilfe von Geschäftsprozessmodellen, dass weder tatsächliche Geschäftsobjekte verarbeitet noch Leistungsverpflichtungen eingegangen oder erfüllt werden. Schuster (Schuster, 2012) bezeichnet dies in seiner nachfolgenden Definition des Begriffs Simulation als „virtuelle Ausführung":

Definition 6.1:
Simulation
*„**Simulation** ist eine Methode, um das Verhalten von Systemen zu untersuchen und vorherzusagen. Simulation beinhaltet die virtuelle Ausführung von Modellen (Simulationsmodellen), die das zu untersuchende System beschreiben. Zur Bewertung des Verhaltens wird das System virtuell über eine definierte Zeitspanne unter Zuhilfenahme von Eingabeparametern ausgeführt. Während der Simulation werden zu untersuchende Parameter und ausführungsrelevante Informationen aufgezeichnet, diese Daten bilden das Simulationsergebnis." (Schuster, 2012, S. 15)*

Werden Geschäftsprozesse mit Petri-Netzen modelliert, so besteht eine Simulation aus virtuellen Schaltvorgängen. Da Zustandsänderungen in Petri-Netzen zu diskreten (also unterscheidbaren) Zeitpunkten erfolgen, ist für diese Arbeit die Simulation diskreter Prozesse relevant. Da aber auch bei der realen Durchführung eines mittels eines Informationsvertraulichkeits- und Datenschutz-Netzes modellierten Geschäftsprozesses die Schaltvorgänge zu diskreten Zeitpunkten stattfinden, ist diese Simulationsbedingung ohne Beschränkung der Allgemeinheit anzunehmen. Im Sinne der Definition ist die Anfangsmarkierung m_0 der Eingabeparameter. Ausgehend von einer Anfangsmarkierung findet dann ein Schaltvorgang beziehungsweise finden dann mehrere Schaltvorgänge statt. Anders ausgedrückt schaltet zunächst eine aktivierte Transition, eventuell schalten danach weitere dann aktivierte Transitionen. Als Teil des Simulationsergebnisses können sowohl die Schaltreihenfolge als auch die sich nach den jeweiligen Schaltungen ergebenden Markierungen festgehalten werden. Ist das Simulationsergebnis aufgrund der Eingabeparameter nicht vom Zufall abhängig, das heißt eindeutig festgelegt, spricht man von einer deterministischen Simulation (Hedtstück, 2013, S. 10). Dies beinhaltet auch, dass die Schaltreihenfolge aufgrund der Anfangsmarkierung m_0 eindeutig feststeht. Dies ist dann der Fall, wenn immer nur eine Transition gleichzeitig aktiviert ist und somit schalten kann. Abbildung 14 zeigt vier Zustände eines Petri-Netzes $\mathrm{N} = (\mathrm{P}, \mathrm{T}, \mathrm{F})$ mit der Menge an Stellen $P = \{1, 2, 3, 4\}$, der Menge an Transitionen $T = \{a, b, c\}$ und der Flussrelation $F =$

$\{(1,a),(a,2),(2,b),(b,3),(3,c)(c,4)\}$. Zeile 1 der Abbildung zeigt das Petri-Netz mit der Anfangsmarkierung, formal beschrieben mit der Funktion $m_0(p) \coloneqq 1\ f\text{ü}r\ p = 1, 0\ sonst$. Nur die Transition a ist aktiviert und kann schalten. Schaltet a, so wird m_0 in m_1 überführt. Dies lässt sich auch als $m_0 \overset{a}{\rightarrow} m_1$ schreiben. Der entsprechende Folgezustand ist in der zweiten Zeile der Abbildung dargestellt. Es folgen weitere Schaltungen: $m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_3$. Die letzte Zeile der Abbildung stellt m_3 dar: $m_3(p) \coloneqq 1\ f\text{ü}r\ p = 4, 0\ sonst$.

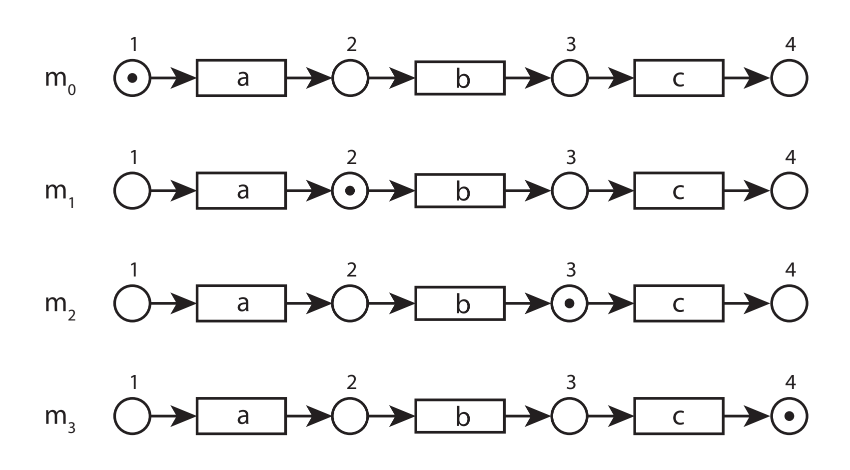


Abbildung 14: Beispiel für eine deterministische Simulation

Steht das Simulationsergebnis, also insbesondere auch die Schaltfolge der Transitionen, aufgrund der Eingabeparameter nicht eindeutig fest und hängt vom Zufall ab, so spricht man von einer stochastischen (das heißt nicht deterministischen) Simulation (Hedtstück, 2013, S. 10). Dies ist beispielsweise dann der Fall, wenn bei einer Markierung m' mehrere Transitionen schalten können. Ein Beispiel dafür sind nebenläufige Transitionen. Abbildung 15 zeigt sechs Zustände von zwei möglichen Schaltfolgen eines Petri-Netzes $\mathrm{N} = (\mathrm{P}, \mathrm{T}, \mathrm{F})$ mit der Menge an Stellen $P = \{1,2,3,4,5,6\}$, der Menge an Transitionen $T = \{a,b,c,d\}$ und der Flussrelation $F = \{(1,a),(a,2),(a,3),(2,b),(3,c),(b,4),(c,5),(4,d),5,d),(d,6)\}$. Die erste Zeile der Abbildung zeigt das Petri-Netz mit der Anfangsmarkierung, ausgedrückt mit der

Funktion $m_0(p) \coloneqq 1\ für\ p = 1, 0\ sonst$. Nur die Transition a ist aktiviert und kann schalten. Schaltet a, so wird m_0 in m_1 überführt. Nun sind die Transitionen b und c aktiviert. Es ist nicht bestimmt, welche Transition zuerst schalten wird, da sie unabhängig voneinander sind (Zimmer, 2001, S. 17). Entweder b schaltet und überführt m_1 in m_2 oder c schaltet zuerst und überführt m_1 in m_{2^*}; die Reihenfolge wird also zufällig festlegt (Zimmer, 2001, S. 17). Mit dem nächsten Zustandsübergang durch Schalten von c oder b wird der Zustand m_3 erreicht. Danach ist die weitere Ausführung deterministisch. Es sind dementsprechend die beiden folgenden Schaltfolgen möglich: 1) $m_0 \overset{a}{\to} m_1 \overset{b}{\to} m_2 \overset{c}{\to} m_3 \overset{d}{\to} m_4$ beziehungsweise 2) $m_0 \overset{a}{\to} m_1 \overset{c}{\to} m_{2^*} \overset{b}{\to} m_3 \overset{d}{\to} m_4$.

Solche nicht deterministischen Simulationen können beispielsweise auch entstehen, wenn ein Geschäftsprozessmodell alternative Pfade durch ein exklusives „Oder" enthält. Sind mehrere Transitionen zur gleichen Zeit aktiviert, und gibt es keine weiteren Bestimmungen, die festlegen, welche Transition als Nächstes schaltet, hängt es vom Zufall ab, welche Transition zuerst schaltet. Es kann festgelegt werden, dass die Schaltwahrscheinlichkeit für jede Transition gleich ist. Es ist aber auch möglich, andere Wahrscheinlichkeiten festzulegen. In jedem Fall zeigt sich jedoch auch eine Schwäche der Simulation: Mit einem Simulationslauf kann nur eine mögliche Schaltfolge untersucht werden, und es ist zunächst nicht bekannt, wie viele Simulationsdurchläufe benötigt werden, um alle möglichen Simulationsergebnisse festzustellen, sofern die Menge der möglichen Simulationsergebnisse überhaupt endlich ist.

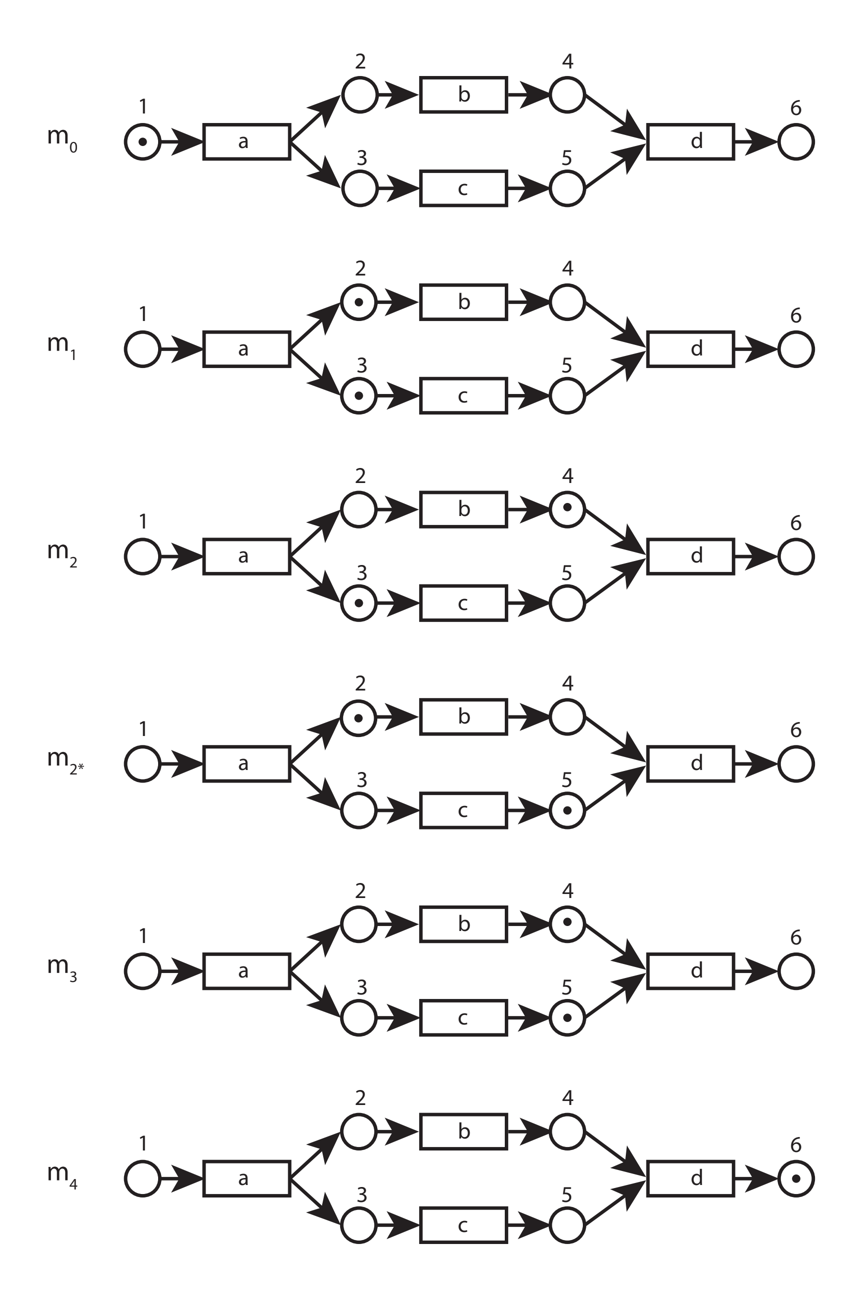


Abbildung 15: Beispiel einer stochastischen Simulation mit zwei möglichen Simulationsergebnissen

Auch wenn diese Herausforderung nicht spezifisch für Informationsvertraulichkeits- und Datenschutz-Netze ist, so ist es dennoch notwendig, für diese eine geeignete Simulationsstrategie zu wählen. Eine Möglichkeit, diese zu finden, ist der Markierungsgraph (auch Erreichbarkeitsgraph genannt). Der Markierungsgraph zu einem Petri-Netz $N = (P, T, F)$ ist abhängig von der Anfangsmarkierung m_0. Die Knoten des Markierungsgraphen sind die von m_0 mit einer beziehungsweise mehreren Schaltungen (Schritten) erreichbaren Markierungen. Die Kanten repräsentieren diese Schritte (Reisig, 2010, S. 31). Gibt es eine Schaltung, die den Zustandsübergang von einer Markierung zu einer anderen ermöglicht, so wird zwischen den Markierungen eine entsprechend gerichtete Kante gezogen und mit dem Namen der schaltenden Transition beschriftet.

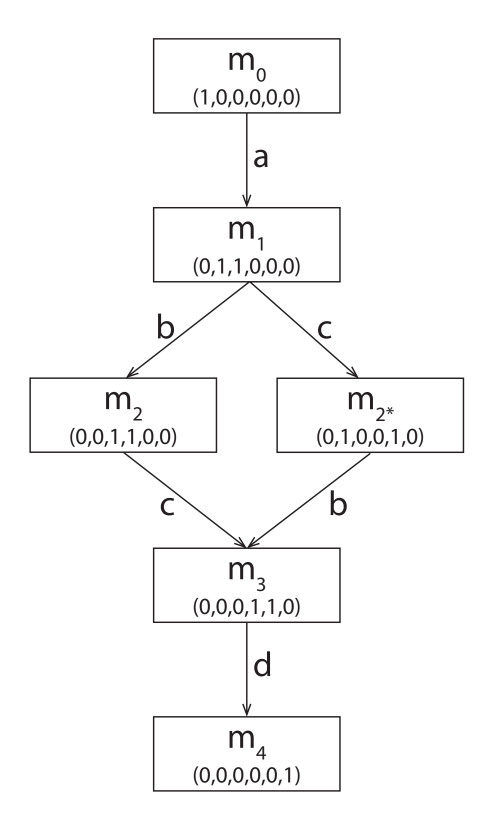


Abbildung 16: Markierungsgraph zum Petri-Netz aus Abbildung 15 mit Anfangsmarkierung m_0

Reisig (Reisig, 2010, S. 32) stellt fest: „Prinzipiell eignet sich der Markierungsgraph eines Systemnetzes als Ausgangspunkt für seine (rechnergestützte) Analyse, sofern nur endlich viele Markierungen erreichbar sind.“ Falls also nur endlich viele Markierungen erreichbar sind, ist der Markierungsgraph ein geeignetes Hilfsmittel für eine zu Informationsvertraulichkeits- und Datenschutz-Netzen passende Simulationsstrategie. Wie bei Desel u. a. (Desel, Oberweis, Zimmer & Zimmermann, 1997) wird nachfolgend ein Konzept der Testentwicklung für Software auf die Simulationsentwicklung für Geschäftsprozesse übertragen. Konkret wird die Simulationsstrategie mithilfe des Markierungsgraphen analog zu Teststrategien für Glass-Box-Tests für Software mithilfe des Kontrollflussgraphen festgelegt. Dabei gibt es die folgenden Überdeckungen bei dem kontrollflussorientierten Softwaretest (Zhu, Hall & May, 1997):

- Knotenüberdeckung: Jeder Knoten des Kontrollflussgraphen muss für eine vollständige Knotenüberdeckung mindestens einmal besucht worden sein.
- Kantenüberdeckung: Jede Kante des Kontrollflussgraphen muss für eine vollständige Kantenüberdeckung mindestens einmal genutzt worden sein. Kantenüberdeckung schließt Knotenüberdeckung mit ein.
- Pfadüberdeckung: Jeder mögliche Pfad vom Startknoten zum Endknoten muss für eine vollständige Kantenüberdeckung mindestens einmal genutzt worden sein. Pfadüberdeckung schließt Kanten- und Knotenüberdeckung mit ein.

Für die Simulation von Informationsvertraulichkeits- und Datenschutz-Netzen ist zunächst festzulegen, ob durch die Simulationsläufe alle möglichen Markierungen mindestens einmal erreicht werden müssen (Knotenüberdeckung) oder ob mindestens das stärkere Kriterium der Kantenüberdeckung (das heißt, jede Kante muss 1 x genutzt worden sein) im Markierungsgraph zu fordern ist. Da die Kanten im Markierungsgraphen die Transitionen des zugrunde liegenden Informationsvertraulichkeits- und Datenschutz-Netzes repräsentieren und diese für

die einzelnen Kenntnisnahmen und Verarbeitungsschritte stehen, wird für die Simulation von Informationsvertraulichkeits- und Datenschutz-Netzen Kantenüberdeckung gefordert.

Es ist auch möglich, dass die Menge der möglichen Simulationsergebnisse unendlich ist, obwohl der Markierungsgraph endlich ist. Dies ist beispielsweise dann der Fall, wenn es im Geschäftsprozessmodell eine oder mehrere Transitionen gibt, die aufgrund einer Schleife beliebig oft ausgeführt werden können, aber wieder zu den gleichen Markierungen führen.

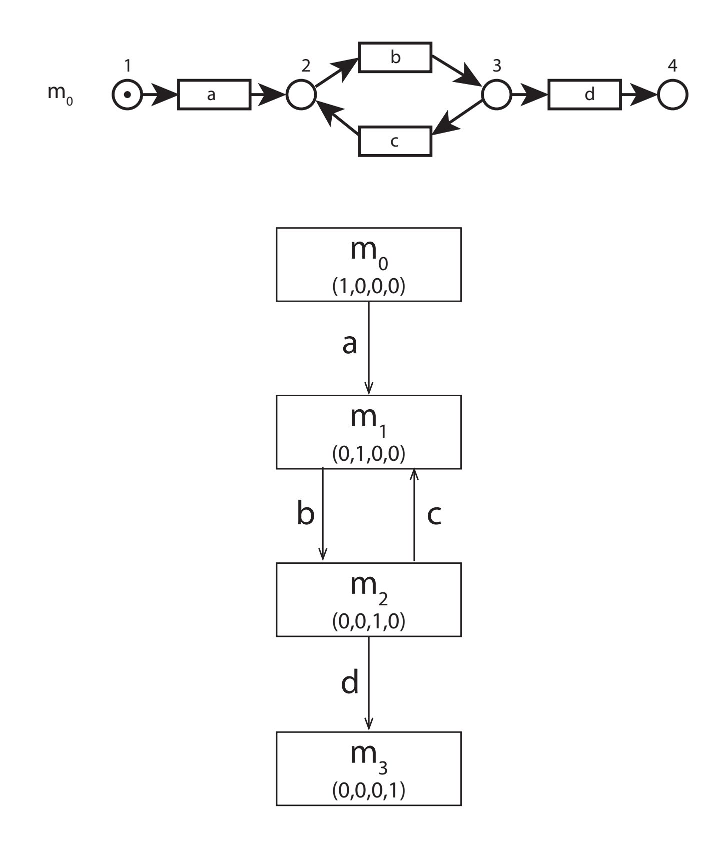


Abbildung 17: Beispiel für ein Petri-Netz mit Anfangsmarkierung m_0, endlichem Markierungsgraphen und unendlicher Menge an möglichen Simulationsergebnissen

Abbildung 17 verdeutlicht dies. Oben ist ein Petri-Netz mit einer Anfangsmarkierung m_0 zu sehen, unten der zugehörige Markierungsgraph. Mit mindestens drei Schaltungen kann der Endzustand m_3 (eine Marke in der 4. Stelle) erreicht werden: $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$. Ein alternativer Pfad, um den Endzustand m_3 zu erreichen, ist $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$. Dabei lässt sich das Schalten von c, b unendlich oft wiederholen; dies verdeutlicht die eckige Klammer mit dem hochgestellten Stern in der nachfolgenden Schaltfolge: $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \left[\overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2\right]^* \overset{d}{\rightarrow} m_3$.

In Informationsvertraulichkeits- und Datenschutz-Netzen ist dies auch möglich. Die Frage ist, ob es ausreichend ist, hier weiterhin nur Kantenüberdeckung zu fordern. Da dadurch alle Transitionen des Informationsvertraulichkeits- und Datenschutz-Netzes geschaltet haben und alle Kanten genutzt wurden (weil alle Markierungen erreicht wurden), kann bereits eine gute Analyseaussage getroffen werden. Die stärkere Forderung der Pfadüberdeckung lässt sich wegen der unendlichen Anzahl an möglichen Pfaden nicht umsetzen und verspricht keinen deutlichen Mehrwert für Informationsvertraulichkeits- und Datenschutz-Netze. Am Beispiel des Netzes aus Abbildung 17 bedeutet dies, dass nach dem Simulationslauf $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$ zwar die Knotenüberdeckung im Markierungsgraph erreicht ist, aber noch keine Kantenüberdeckung. Daher muss ein erneuter Simulationslauf ausgeführt werden: $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$. Damit ist auch die Kantenüberdeckung erreicht. Es können nun sowohl Aussagen zu allen Markierungen (jede wurde mindestens einmal erreicht) als auch zu allen Transitionen (jede hat mindestens einmal geschaltet) getroffen werden. Die nicht deterministische Simulation hätte beispielsweise auch $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$ oder $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{c}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$ als ersten Lauf durchführen können und wäre dann aufgrund der erreichten Kantenüberdeckung beendet. Eine Pfadüberdeckung kann in diesem Beispiel gar nicht erreicht werden, weil die Anzahl an Pfaden in dem Beispiel unendlich ist.

Pfadüberdeckung wird aus den genannten Gründen nicht für die Simulation von Informationsvertraulichkeits- und Datenschutz-Netzen gefordert. Stattdessen wird Kantenüberdeckung (diese schließt Knotenüberdeckung ein) gefordert.

Eine andere Problematik entsteht, wenn die unendliche Menge an Simulationsergebnissen aufgrund eines unendlichen Markierungsgraphen entsteht. Dieses Problem ist als State Explosion Problem (Valmari, 1998) bekannt. Abbildung 18 zeigt ein entsprechendes Petri-Netz mit Anfangsmarkierung m_0.

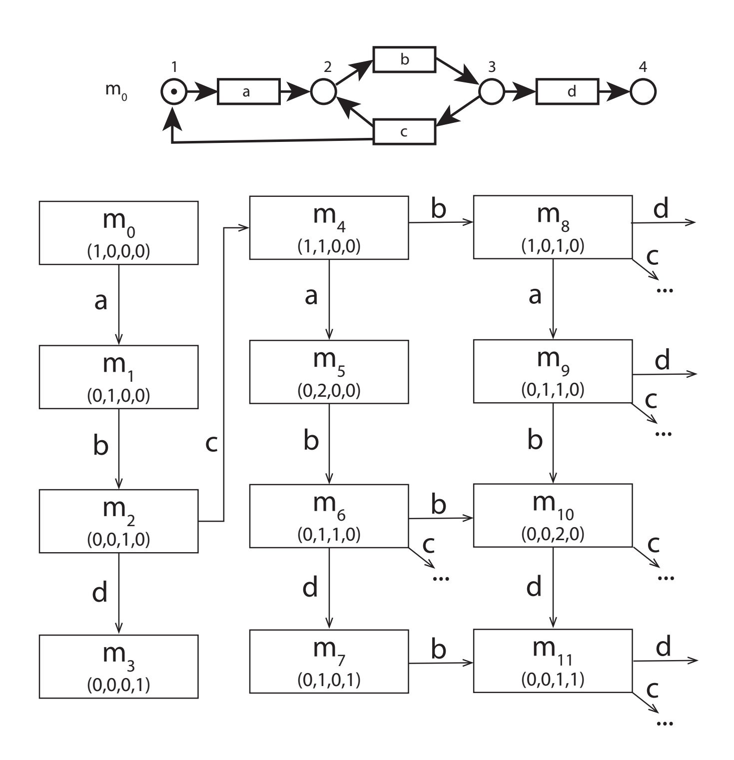


Abbildung 18: Petri-Netz mit Anfangsmarkierung m_0 mit resultierendem unendlichem Markierungsgraphen, ausschnittsweise dargestellt

Das Netz kann beispielsweise mit der Schaltfolge $m_0 \overset{a}{\rightarrow} m_1 \overset{b}{\rightarrow} m_2 \overset{d}{\rightarrow} m_3$ terminieren; es sind abhängig von den schaltenden Transitionen jedoch auch unendlich viele wei-

tere Markierungen möglich. Sowohl der Markierungsgraph als dadurch auch die mögliche Menge der Simulationsergebnisse ist unendlich. Daher ist es nicht möglich, mit einer endlichen Anzahl an Simulationsläufen Kantenüberdeckung zu erreichen.

6.3 ICPN-Sim

Aufbauend auf den beschriebenen Simulationsverfahren und Simulationsstrategien für Workflow-Netze wird nachfolgend das Simulationsverfahren für Informationsvertraulichkeits- und Datenschutz-Netze ICPN-Sim beschrieben, wobei die Einschränkungen der Workflow-Eigenschaften gelten. Das Verfahren besteht aus den folgenden Schritten:

1. Bildung des Markierungsgraphen des zugrunde liegenden Workflow-Netzes bezüglich der festgelegten Anfangsmarkierung. Dabei werden die im Informations- und Datenschutz-Workflow-Netz zusätzlich vorhandenen Restriktionen (wie beispielsweise strengere Schaltbedingungen) nicht berücksichtigt.
2. Simulation des Informations- und Datenschutz-Workflow-Netzes mit der Anfangsmarkierung. Dabei wird, sofern er endlich ist, der Markierungsgraph verwendet, und es wird eine Kantenüberdeckung angestrebt. Für jeden Simulationslauf gilt:
    a. Protokollieren des simulierten Informations- und Datenschutz-Workflow-Systems (das heißt Informations- und Datenschutz-Workflow und Anfangsmarkierung)
    b. Feststellen der aktivierten Transitionen
        i. Ist genau eine Transition aktiviert, so wird diese Transition geschaltet und der Schaltvorgang entsprechend protokolliert.
        ii. Ist mehr als eine Transition aktiv (das heißt, es dürfen mehrere Transitionen schalten), wird die Transition ausgewählt, die ausgehend von dieser Markierung noch nicht

geschaltet hat. Sind dies mehrere Transitionen, wird unter diesen eine zufällig ausgewählt und die Notwendigkeit eines weiteren Simulationslaufs mit Besuch dieses Zustands (beispielsweise durch Wiederholen der bisherigen Schaltungen) vermerkt.
Die ausgewählte Transition wird geschaltet und der Schaltvorgang wird protokolliert.

   iii. Sind keine Transitionen aktiv, ist dieser Simulationslauf beendet. Der Endzustand wird protokolliert.

   c. Solange der Simulationslauf nicht beendet wurde, b wiederholen; sonst weiter zu d.
   d. Schlusszustand des Simulationslaufs protokollieren.

3. Überprüfung, welche Kanten bei den bisherigen Simulationsläufen nicht genutzt wurden. Die ungenutzten Kanten könnten aufgrund der Eigenschaften der Informationsobjekte nicht genutzt worden sein, weil die zugehörige Transition nicht aktiv war. Es ist zu überprüfen, ob sich in einem weiteren Simulationslauf im Rahmen des modellierten Prozesses und der Anfangsmarkierung die Eigenschaften so wählen lassen, dass die Kante genutzt werden kann beziehungsweise die zugehörigen Transitionen schalten können. Hierzu kommen nur Eigenschaften infrage, die erst zur Laufzeit dynamisch festgelegt werden (beispielsweise eine Kundeneingabe).

Die Vorgehensweise zur Simulation wird in Abbildung 19 zusammengefasst. Durch das folgende Unterkapitel werden die Aktivitäten zur Protokollierung näher spezifiziert.

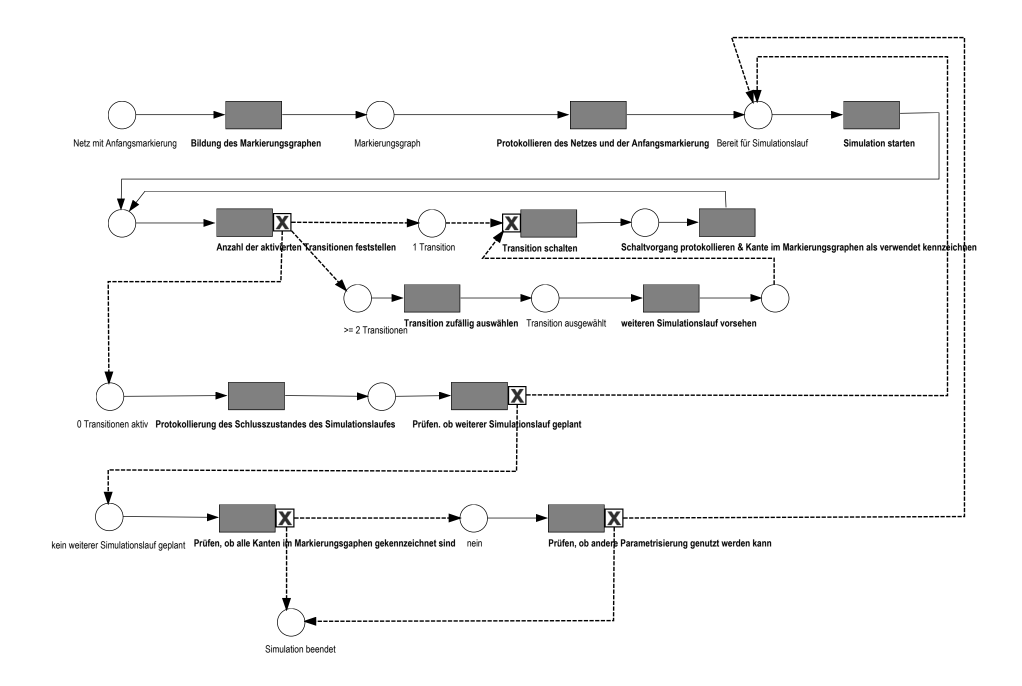


Abbildung 19: Darstellung des Simulationsablaufes

6.4 Simulationsprotokoll ICPN-Trace

Die Analysemöglichkeiten eines oder mehrerer Simulationsläufe werden entscheidend von dem währenddessen erzeugten Simulationsprotokoll beeinflusst. Während der Simulation werden die Ereignisse aufgezeichnet und abgespeichert, wodurch später eine vielfältige Analyse möglich ist (Gruhn & Haack, 1995). Für Informationsvertraulichkeits- und Datenschutz-Netze soll während einer Simulation daher festgehalten werden:

Zunächst enthält das Protokoll alle Informationen, um das simulierte System (Informationsvertraulichkeits- und Datenschutz-Netz) eindeutig zu beschreiben. Dazu werden protokolliert:

- Informationsvertraulichkeits- und Datenschutz-Netz (wie simuliert): Da sich ein Informationsvertraulichkeits- und Datenschutz-Netz als Modell eines Geschäftsprozesses im Rahmen des Geschäftsprozessmanagements verändern kann (in der Phase Prozessdesign des Business Process Management Lifecycle (de Morais, Kazan, Pádua & Costa, 2014)), ist es notwendig, entweder die Version im Protokoll eindeutig zu identifizieren oder das gesamte Informationsvertraulichkeits- und Datenschutz-Netz in das Protokoll aufzunehmen. Hierzu bietet sich der XML-Dialekt Petri-Net-Markup-Language (PNML) an (vgl. ISO/IEC 15090-2, 2011). Der Standard lässt Freiheitsgrade zu, um in sogenannten Tool-Specific-Tags für Informationsvertraulichkeits- und Datenschutz-Netze spezifische Informationen abzubilden.
- Anfangsmarkierung: Die Belegung der Stellen des Informationsvertraulichkeits- und Datenschutz-Netzes durch Marken ist festzuhalten. Jede Marke erhält dafür eine eindeutige Identifikationsnummer (ID). Die IDs der Anfangsmarkierung werden als ganzzahlig, beginnend bei 1 aufsteigend, vergeben. Da für die Analyse der Informationsvertraulichkeits- und Datenschutz-Netze die Workflow-Eigenschaften gefordert werden, gibt es nur eine Marke in der Anfangsmarkierung. In jedem Fall ist je Marke auch festzuhalten, ob die initiale Marke personenbezogene Daten enthält ($CPD = wahr$) oder nicht ($CPD = falsch$), und für welche Zwecke eine Verarbeitung gestattet ist.

Für jeden Schritt – das heißt das Schalten einer Transition bei der Simulation eines Informationsvertraulichkeits- und Datenschutz-Netzes – sind die nachfolgenden Informationen für eine spätere Analyse des Simulationsergebnisses festzuhalten.

- Aktivierte Transitionen: Welche Transitionen des Informationsvertraulichkeits- und Datenschutz-Netzes sind aktiviert, das heißt können schalten?
- Schaltende Transition: Festgehalten wird, welche Transition schaltet.

- Je Eingangskante wird die ID der konsumierten Marke (= des Informationsobjekts) festgehalten. Für jede konsumierte Marke wird protokolliert:
    - welche Informationsvertraulichkeit mit der Marke verknüpft ist,
    - welches Mengensystem $ROO(i)$ mit der Marke verknüpft ist und somit, welche Mengen den Zugriff auf die Information *i* gestatten,
    - ob die Marke personenbezogene Informationen enthält ($CPD = wahr$) oder nicht ($CPD = falsch$) und
    - welche Verarbeitungszwecke $L(i)$ gestattet sind.
    - Je Eingangskante kann auch ein Zweck der Verarbeitung festgelegt sein. Daher ist je Eingangskante für die konsumierte Marke (ID) der Zweck zu protokollieren. Später kann solch für ein Informationsobjekt, das heißt eine Marke, festgestellt werden, welche Zwecke für den Verarbeitungsverlauf benötigt wurden (Einwilligung notwendig).
- Außerdem wird protokolliert, welche Ressourcen (verknüpft mit der Transition) daran beteiligt sind. Je beteiligter Ressource wird zudem die Menge aller Rollen der Ressource $ROR(r)$ festgehalten. Da in Informationsvertraulichkeits- und Datenschutz-Netzen die Rollenzuweisung an Ressourcen statisch ist, kann dies für alle an der gesamten Ausführung beteiligten Rollen an einer Stelle des Logs gespeichert werden. Ist die beteiligte Ressource beim Schalten der Transition dort bereits gelistet, muss nichts getan werden (die Beteiligung der Ressource an der schaltenden Transition wurde bereits festgehalten). Ist die beteiligte Ressource noch nicht gelistet, müssen die Rollen der Ressource an der zentralen Stelle ergänzt

werden (dass die Ressource am Schaltvorgang beteiligt war, ist bereits festgehalten).

- Zur späteren Analyse der Datenminimierung wird protokolliert, welche personenbezogenen Daten benötigt wurden (Menge $D(t)$). Diese Menge ist zwar je Transition in Informationsvertraulichkeits- und Datenschutz-Netzen statisch, es vereinfacht jedoch die spätere Analyse, wenn die Information während des Simulationsschritts unmittelbar protokolliert wird.
- Je Ausgangskante werden die produzierten Marken protokolliert. Dazu erhält jede Marke eine ID. Wenn eine Transition genau eine Eingangskante hat, genau eine Marke konsumiert wurde und die Transition genau eine Marke produziert (genau eine Ausgangskante), wird die ID der Marke beibehalten.
  Werden mehrere Marken konsumiert, wird überprüft, ob ihre IDs einen gemeinsamen Beginn haben (beispielsweise 1.1 und 1.2, gemeinsamer Beginn 1). Dabei muss die ID bis auf die letzte Stelle (hinter dem letzten Punkt) übereinstimmen. Falls ja, wird überprüft, ob es andere Marken mit dem gemeinsamen Beginn gibt. Wenn dies nicht der Fall ist, wird der gemeinsame Beginn (ohne den letzten Punkt) zur neuen ID. In allen anderen Fällen wird eine neue einmalige ID vergeben.
  Werden mehrere Marken produziert, so wird ihre ID durch Anhängen eines Punkts und einer je Marke aufsteigenden Nummer (ab der Nummer 1) gebildet.
  Die Bildung der IDs ist in Listing 1 wiedergegeben.

- Die jeweiligen Eigenschaften je produzierter Marke werden festgehalten:
  - Informationsvertraulichkeit der Marke,
  - Mengensystem $ROO(i)$ mit den Mengen, die den Zugriff auf die Information i gestatten,

- gestattete Zwecke, die aufgrund der eingehenden Marke (falls eine Marke mit dem gleichen Typ eingeht) und der Inschrift an der Ausgangskante festgelegt beziehungsweise verändert werden,
- Feststellung, ob die Marke personenbezogene Informationen enthält ($CPD = wahr$) oder nicht ($CPD = falsch$). Dies kann entweder unverändert (nur, falls eine Marke mit dem gleichen Typ eingeht) oder durch die Ausgangskante festgelegt sein.

Protokollierung des Endzustands:

- Schlussmarkierung: Die Belegung der Stellen des Informationsvertraulichkeits- und Datenschutz-Netzes durch Marken ist festzuhalten. Je Marke ist auch festzuhalten, ob die initiale Marke personenbezogene Daten enthält ($CPD = wahr$) oder nicht ($CPD = falsch$) und für welche Zwecke eine Verarbeitung gestattet ist.

Das Simulationsprotokoll ist in einem geeigneten Format zu speichern. Da die Petri-Netze bereits in PNML (ein XML-Derivat) gespeichert werden, wurde für die Speicherung der Simulationsergebnisse ebenfalls XML als Format festgelegt.

```
public  String[]  markenIDsAusgang(String[]  markenIDsEingang,  int  anzahlAusgangskanten,
String[] aktuelleMarkenIDs, int naechsteMarkenID) {

    String stammID = ""; //stammID für Ausgangsmarken
    String[] markenIDsAusgang = new String[anzahlAusgangskanten];
    int anzahlEingangskanten = markenIDsEingang.length;

    if (anzahlEingangskanten == 1 && anzahlAusgangskanten == 1) {
        //Das Array markenIDsEingang enthält folglich 1 Element und wird weiter verwendet
        markenIDsAusgang = markenIDsEingang;
        return markenIDsAusgang;
    }

    if (anzahlEingangskanten == 1) {
        //Das  Array  markenIDsEingang  enthält  folglich  1  Element  und  wird  als  Stamm-ID
verwendet
        stammID = markenIDsEingang[0];
    }

    //Mehrere Marken konsumiert
    if (anzahlEingangskanten >= 1) {
        //StammID festlegen
        boolean gemeinsamerBeginn = true;
        String[] markenIDEingang0 = markenIDsEingang[0].split(".");
        for (int i = 1;
            (i <= anzahlEingangskanten && gemeinsamerBeginn); i++) {
            String[] markenIDEingangI = markenIDsEingang[i].split(".");
            if (markenIDEingang0.length == markenIDEingangI.length) {
                for (int k = 0; k <= markenIDEingang0.length - 1; k++) {
                    if (markenIDEingang0[k] != markenIDEingangI[k]) {
                        gemeinsamerBeginn = false;
                    }
                }
            } else {
                gemeinsamerBeginn = false;
            }
        }
        if (gemeinsamerBeginn) {
            for (int i = 0; i < markenIDEingang0.length - 1; i++) {
                stammID = stammID + "." + markenIDEingang0[i];
            }
            //prüfen ob StammID aktuell in Gebrauch
            for (int i = 0; i < aktuelleMarkenIDs.length; i++) {
                if (aktuelleMarkenIDs[i].startsWith(stammID)) {
                    stammID = naechsteMarkenID + ".";
                }
            }

        }
    }

    if (anzahlAusgangskanten == 1) {
        markenIDsAusgang[0] = stammID;
        return markenIDsAusgang;
    }
    for (int i = 0; i <= anzahlAusgangskanten; i++) {
        markenIDsAusgang[i] = stammID + "." + (i + 1);
    }
    return markenIDsAusgang;
}
```

Listing 1: Berechnung der Marken-IDs für die ausgehenden Kanten in Java

6.5 Auswertung der Simulation

Um aus einer Simulation Erkenntnisse gewinnen zu können, werden Kennzahlen zu wichtigen Eigenschaften des Prozesses erhoben, das heißt aus dem Simulationsergebnis abgeleitet.

Im Folgenden wird aufgezeigt, wie das Simulationsergebnis die in Kapitel 6.1 gestellten Fragen beantworten kann.

Frage 1 betrachtet die Auswirkungen der neuen Informations-vertraulichkeits- und Datenschutz-Anforderungen auf die Geschäftsprozesse. Die konkret gestellte Frage der Ausführbarkeit kann beantwortet werden, indem die einzelnen Simulationsläufe mit dem zuvor erstellten Markierungsgraphen verglichen werden. Ziel ist es, Transitionen zu finden, die nicht schalten können, das heißt Aktivitäten, die nicht länger ausgeführt werden können. Sind diese Aktivitäten identifiziert, kann der Modellierungsexperte die Ursachen überprüfen und ggf. den Ablauf oder beispielsweise die Ressourcenzuweisung anpassen.

Frage 2 führt dementsprechend zu einer verbesserten Ressourcenallokation, indem betrachtet wird, welche Vertrauenswürdigkeit Ressourcen mindestens besitzen müssen, um an einem Prozess beziehungsweise an einer Aktivität wie vorgesehen mitzuwirken. Schwieriger kann die Ressourcenallokation bei rollenbasierter Informationsvertraulichkeit umgesetzt werden. Hier wird die minimale Rollenkombination, also die Menge an Rollen, die eine Ressource mindestens benötigt, um eine Aktivität ausführen zu dürfen, gesucht. Im Rahmen der Simulation und ihrer Auswertung kann festgestellt werden, welche Rollenkombinationen jeweils hinreichend zur Ressourcenallokation wären. Die „minimale" Rollenkombination muss jedoch nicht die Menge mit der kleinsten Anzahl an Elementen sein. Gesucht ist vielmehr die „unkritischste" Menge, bezogen auf die weiteren Möglichkeiten der Rollen. Das Modell und die Simulation können aber nur die Frage beantworten, welche Mengen berechtigt sind. Da – betrachtet man nur ein Modell – nicht klar ist, welche Berechtigungen diese Rollen sonst haben, kann nicht geklärt werden, wie kritisch sie sind. Bis alle

Modelle eines Unternehmens zur Beantwortung dieser Frage herangezogen werden können, muss diese Frage durch den Fachexperten beziehungsweise Modellierer beantwortet werden.

Die dritte Frage betrifft den Datenschutz. Eine Forderung ist die Datenminimierung. Mithilfe des Simulationsprotokolls kann festgestellt werden, welche Daten für die einzelnen Aktivitäten eines Prozesses benötigt werden; anschließend kann die Datenerfassung entsprechend angepasst werden.

Dies führt zur nächsten Frage: Wenn es mehrere Möglichkeiten gibt, ein Ziel zu erreichen, welcher ist dann der datensparsamste Pfad? Diese Frage kann durch den Vergleich der verschiedenen Simulationsläufe beantwortet werden. Natürlich gibt es noch weitere Kriterien wie beispielsweise Laufzeit und Kosten, um einen Pfad zu bewerten. Jedoch kann mithilfe der Informationsvertraulichkeits- und Datenschutz-Netze sowie ihrer Simulation das Kriterium der Datensparsamkeit bewertet werden.

Mithilfe des Simulationsprotokolls kann auch die fünfte Frage beantwortet werden: Werden die Daten hinsichtlich ihrer Zweckbindung verarbeitet, oder werden beispielsweise Einwilligungen für Zwecke eingeholt, die gar nicht benötigt werden?

Für die Auswertung des Simulationsprotokolls stehen aufgrund seines XML-Formats verschiedene Abfragesprachen wie beispielsweise XQuery zur Verfügung (Becher, 2009).

7 Die PriCon4BPM-Methode

In den vorangegangenen beiden Kapiteln wurde eine Erweiterung für Petri-Netze vorgestellt, um eine Modellierung von Aspekten der Informationsvertraulichkeit und des Datenschutzes zu ermöglichen. Es wurden auch Verfahren vorgestellt, um die so beschriebenen Geschäftsprozesse – teilweise mittels Simulation – analysieren zu können.

In diesem Kapitel wird eine Methode vorgestellt, welche mithilfe dieser Spracherweiterung und Analysemöglichkeiten eine systematische Betrachtung von Aspekten der Informationsvertraulichkeit und des Datenschutzes ermöglicht. Daher wurde der Name „PriCon4BPM-Methode“ gewählt. Er setzt sich aus den folgenden Komponenten zusammen:

- *Pri* für *Privacy* (Datenschutz)
- *Con* für *Confidentiality* (Vertraulichkeit)
- *4* für *for* (für)
- *BPM* für *Business Process Management* (Geschäftsprozessmanagement)

7.1 BPM-LifeCycle-Management

„Methoden sind die Vorschriften, wie planmäßig [d. h. auch systematisch] nach einem bestimmten Prinzip (oder einer Kombination von Prinzipien) zur Erreichung festgelegter Ziele vorzugehen ist.“ (Leimeister, 2015, S. 260f.). Nach Brinkkemper (Brinkkemper, 1996) geht es beim ingenieurmäßigen Entwickeln von Methoden darum, neue Methoden zu entwerfen beziehungsweise zu konstruieren und vorhandene Methoden anzupassen. Das trifft nicht nur auf Methoden, sondern auch auf ihre Komponenten (also beispielsweise auf Aktivitäten, Sprachen und Techniken) zu. Demgemäß ist

es sinnvoll zu prüfen, welche Methoden und welche Komponenten angepasst werden können und für welche Herausforderungen ganz neue Lösungen zu entwickeln sind.

Da sowohl Datenschutz als auch Informationsvertraulichkeit mit der PriCon4BPM-Methode innerhalb des Geschäftsprozessmanagements betrachtet werden sollen, ist es zunächst sinnvoll zu prüfen, welche Bestandteile existierender Methoden zum Geschäftsprozessmanagement adaptiert werden können. De Morais u. a. (de Morais, Kazan, de Pádua & Costa, 2014) haben systematisch verschiedene Darstellungen des Lebenszyklus von Geschäftsprozessen betrachtet. Dabei wurden sowohl sechs begleitende Aktivitäten im Lebenszyklus als auch neun Aktivitäten zur initialen Planung beziehungsweise späteren Analyse von Geschäftsprozessen identifiziert. Abgeleitet von de Morais u. a. (de Morais u. a., 2014) werden hier in Abbildung 20 diese sechs Phasen des Lebenszyklus dargestellt.

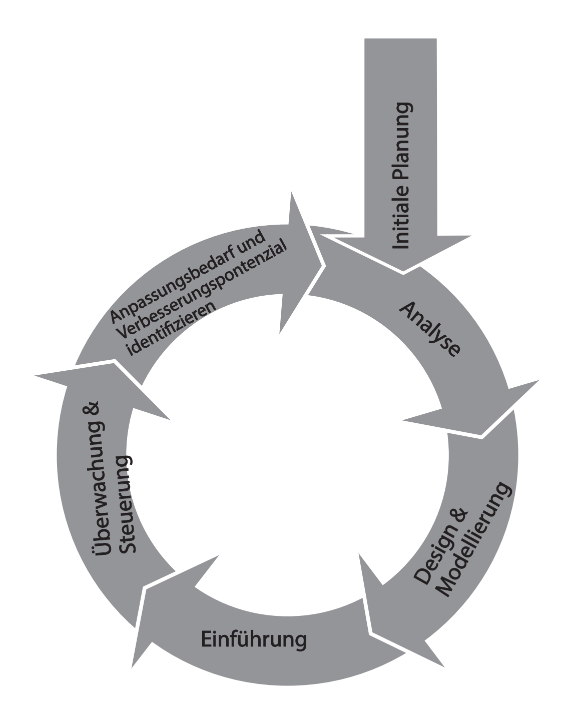


Abbildung 20: Lebenszyklusphasen des Geschäftsprozessmanagements

Dabei fällt auf, dass in keiner der von de Morais u. a. (de Morais u. a., 2014) analysierten Darstellungen ein Austritt aus dem Zyklus skizziert ist. Einen solchen Austritt aus dem Zyklus gibt es in der Praxis durchaus, beispielsweise bei Verlagerung der Geschäftsaktivität oder Geschäftsaufgabe. Ebenfalls fällt auf, dass in allen grafischen Darstellungen ein Kreislauf beschrieben ist, der nach Design und Modellierung die Einführung und Nutzung des Prozesses vorsieht. Es gibt weder skizzierte Rücksprünge noch Phasen des Tests.

Da sowohl Datenschutz als auch Informationsvertraulichkeit nicht nur reine Geschäftsprozesse im Sinne der Ablauforganisation betreffen, sondern in eine Aufbauorganisation eingebettet sind, wurden Informationsvertraulichkeits- und Datenschutz-Netze so gestaltet, dass eine eventuell notwendige Beachtung von aufbauorganisatorischen und Datenstrukturaspekten integriert erfolgen kann. Daher wird hier auch die Horus-Methode betrachtet, da diese bereits eine integrierte Modellierung verschiedener Aspekte vorsieht. Diese gliedert sich in eine Vorbereitungsphase und drei Hauptphasen (Schönthaler, Vossen, Oberweis & Karle, 2012, S. 84 f.):

- Phase 0: Vorbereitungsphase
- Phase 1: Strategie- und Architekturphase
- Phase 2: Geschäftsprozessanalysephase
- Phase 3: Anwendungsphase

Die Geschäftsprozessanalyse besteht aus fünf Hauptaktivitäten, in der Horus-Methode als Verantwortungsbereiche bezeichnet (Schönthaler u. a., 2012, Abbildung 4.14):

1. Strukturelle Analyse zur Definition des Objektmodells und der Geschäftsregeln
2. Ablaufanalyse, entweder auf Basis von Ereignissen oder Anwendungsszenarien
3. Analyse der Organisationsstruktur zur Ermittlung von Rollen und Verantwortlichkeiten

4. Kennzahlenanalyse
5. Risikoanalyse

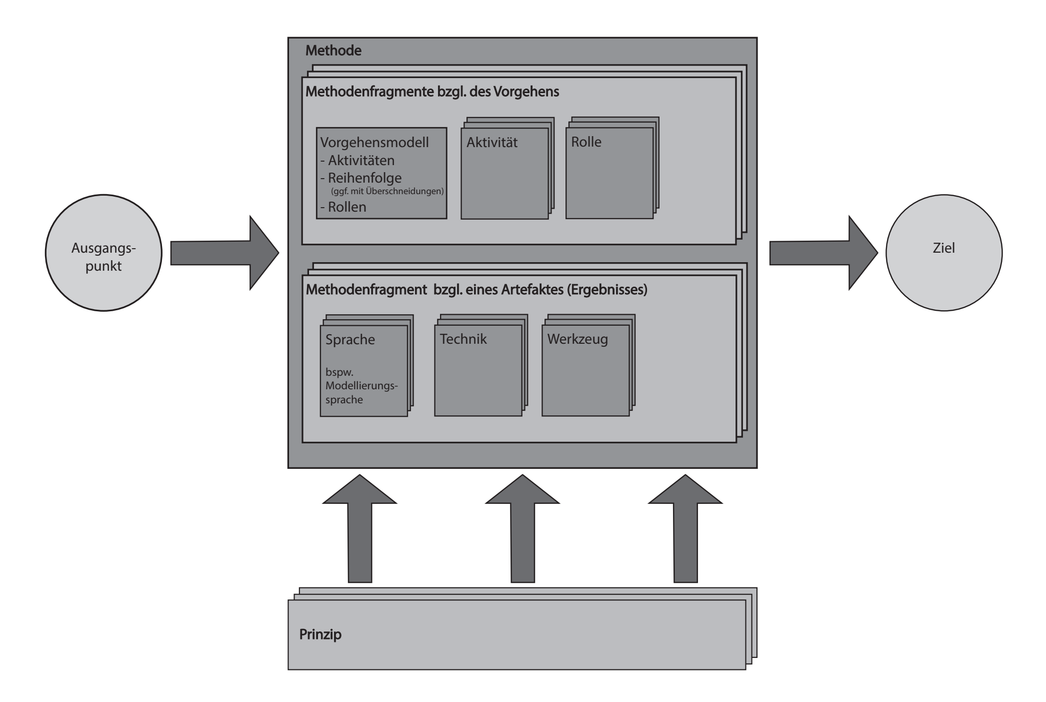


Abbildung 21: Ziel und Bestandteile einer Methode

7.2 Eigene Methode

Methoden bestehen aus verschiedenen Komponenten (Abbildung 21; vgl. Brinkkemper, 1996; Winter, 2003). Um die Methode PriCon4BPM zu entwickeln, werden daher zunächst die einzelnen Komponenten der Methode beschrieben. Hierbei werden ins-

besondere Komponenten, die für diese Methode neu entstehen beziehungsweise angepasst werden müssen, erläutert. Dabei wird zunächst mit den **Aktivitäten** begonnen, und teilweise werden bereits **Techniken** aufgezählt:

- Festlegung des Ziels des Geschäftsprozesses. Diese Aktivität gibt es als Artefakt „Zielmodell der Phase 1“ auch in der Horus-Methode (Schönthaler u. a., 2012, Abbildung 4.10) beziehungsweise als Aktivität „Validate Strategic Direction“ (strategische Ausrichtung überprüfen) bei de Morais u. a. (de Morais u. a., 2014). Die später festzulegenden Zwecke der Datenverarbeitung sollten nicht im Widerspruch zu dem Ziel stehen.
- Sammeln der Aktivitäten des Geschäftsprozesses. Dazu können verschiedene Techniken wie beispielsweise Brainwriting (VanGundy, 1984) verwendet werden, oder auch existierende Prozessbeschreibungen (vom bisherigen Prozess bei einem Redesign von Prozessen) oder von Standardmodellen für bestimmte Aufgaben herangezogen werden.
- Je gesammelter Aktivität:
    - Die notwendigen Informationsobjekttypen zur Ausführung der Aktivität bestimmen. Dabei sind alle Arten von Informationsobjekttypen – sowohl personenbezogene Daten als auch andere – einzubeziehen.
        - Je Informationsobjekttyp prüfen, ob die Informationen bereits vor der Ausführung des Geschäftsprozesses in der Organisation vorliegen oder im Rahmen des Prozesses erhoben werden müssen. Falls die Informationen noch erhoben werden müssen und dafür noch keine Aktivität vorgesehen ist, ist die Sammlung der Aktivitäten um eine entsprechende Aktivität zu ergänzen.
        - Prüfen, ob personenbezogene Daten verarbeitet werden sollen und – falls ja – Festlegen des Zwecks der Aktivität hinsichtlich der Verarbeitung dieser personenbezogenen

Daten. Der Zweck ist später entsprechend an der Eingangskante der Aktivität zu notieren.

- Prüfen, ob es sich um eine spezielle Aktivität zur Einhaltung datenschutzrechtlicher Notwendigkeiten wie beispielsweise die Einholung einer zweckbezogenen Erlaubnis zur Verarbeitung von personenbezogenen Daten oder die Erledigung des Zwecks der Datenverarbeitung handelt. Bei diesen Aktivitäten müssen später die Ausgangskanten entsprechend beschriftet werden. Das bedeutet: Entweder muss eine Menge LA vermerkt werden, um Zwecke hinzuzufügen (beispielsweise wenn eine Erlaubnis für diese Zwecke eingeholt wurde), oder es ist eine Menge LD hinzuzufügen, um Zwecke zu entfernen (beispielsweise wenn Zwecke durch Zweckerfüllung erledigt sind), oder es kann alternativ auch eine Menge LN angegeben werden, um für ein Informationsobjekt eine ganz neue Menge an erlaubten Verarbeitungszwecken zu definieren.
- Festlegen, welche Ressourcen (intern und/oder extern) an der Aktivität beteiligt sein sollen.
- Festlegen, ob und – wenn ja – welche Informationsobjekttypen durch die Aktivität neu erzeugt werden.

- Je Informationsobjekttyp: Prüfen, ob der Informationsobjekttyp schützenswert ist, und – wenn ja – Festlegen der rollenbasierten Informationsvertraulichkeit durch Festlegen der berechtigten Rollenkombinationen – soweit eine statische Festlegung möglich ist.
- Ordnen der Aktivitäten zu einem Geschäftsprozess (Ablauforganisation) und Erzeugung von Stellen. Dabei ist zu beachten, dass die notwendigen Informationsobjekttypen bereitgestellt werden müssen, die entsprechend mit den Eingangsstellen verknüpft sein müssen. Eine Datenstruktur mit fester semantischer Logik ist hier für eine präzise Beschreibung des Geschäftsprozesses erforderlich.

- Je Ressource: Bestimmen der Rollenzugehörigkeit (hinsichtlich der rollenbasierten Informationsvertraulichkeit).
- Nach den vorbereitenden Aktivitäten kann das Informationsvertraulichkeits- und Datenschutz-Netz erstellt werden. Hierzu müssen die Aktivitäten logisch geordnet und ihre Abhängigkeiten berücksichtigt werden. Außerdem sind Stellen zu formulieren, und soweit möglich und notwendig, mit Informationsobjekttypen zu verknüpfen. Zudem müssen bereits vorgemerkte Kantenbeschriftungen, beispielsweise bezüglich der Verarbeitungszwecke einer Transition, vorgenommen werden.
- Simulation/Analyse (teilweise durch Auswertung des Simulationsergebnisses) des Geschäftsprozesses hinsichtlich Datenminimierung, Einhaltung der Zweckbindung und Gewährleistung der Informationsvertraulichkeit. Dadurch sind auch die Kontrollfragen aus Kapitel 3.4.5 zu beantworten:
    - Sind die personenbezogenen Daten erforderlich, um den Zweck zu erreichen?
    - Tragen die Daten zur Erreichung des Zweckes bei?
    - Ist es möglich, den Verarbeitungszweck ohne die Daten (evtl. mit weniger Daten oder mit anonymisierten Daten) zu erreichen?

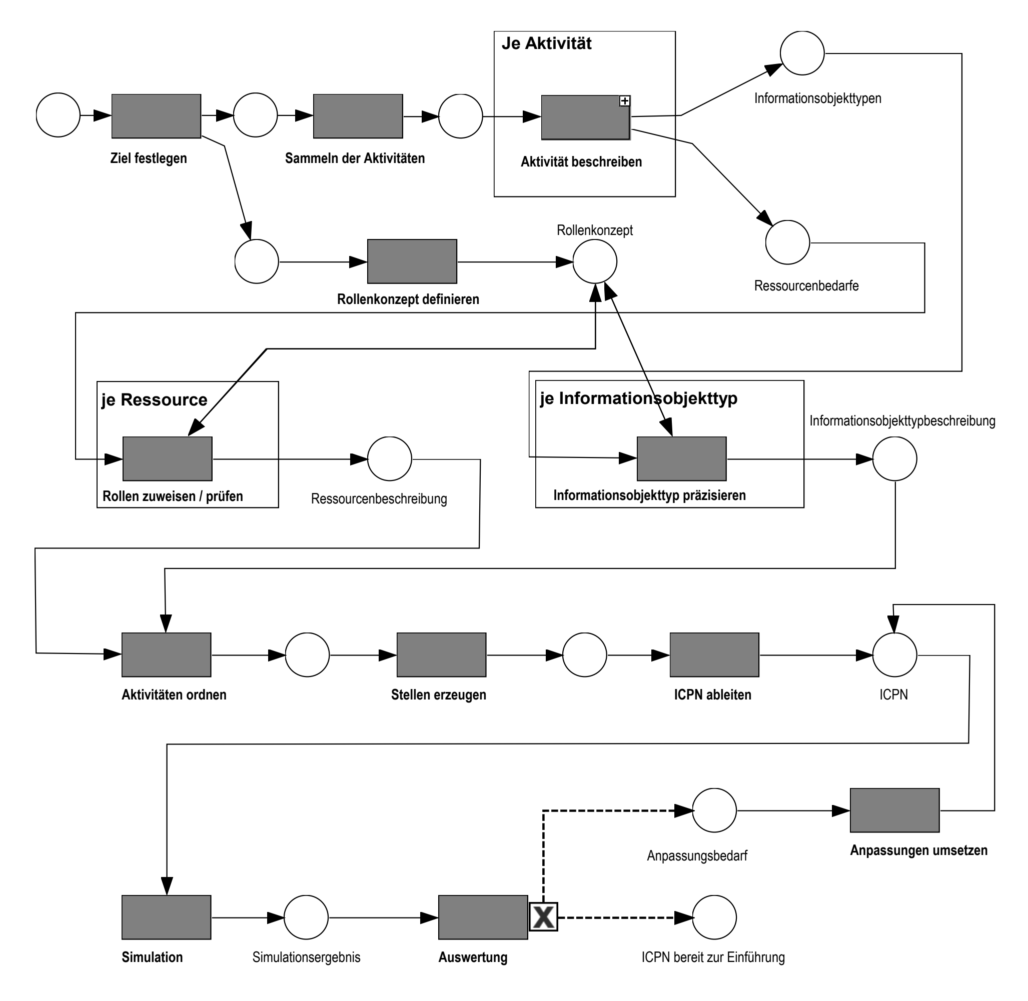


Abbildung 22: Ausschnitt aus dem Vorgehensmodell der PriCon4BPM-Methode

Die Abbildung 22 zeigt die Aktivitäten, geordnet als **Vorgehensmodell**. Dabei bedeutet ein zusätzlicher Kasten um eine Aktivität (Transition) herum, dass der Kasten für mehrere Instanzen, beispielsweise an Ressourcen oder Informationsobjekttypen, durchlaufen wird; der Teilprozess wird genau einmal an jeder Kante betreten, für n ($n \geq 1$) Instanzen ausgeführt und danach genau ein Mal an jeder Kante verlassen.

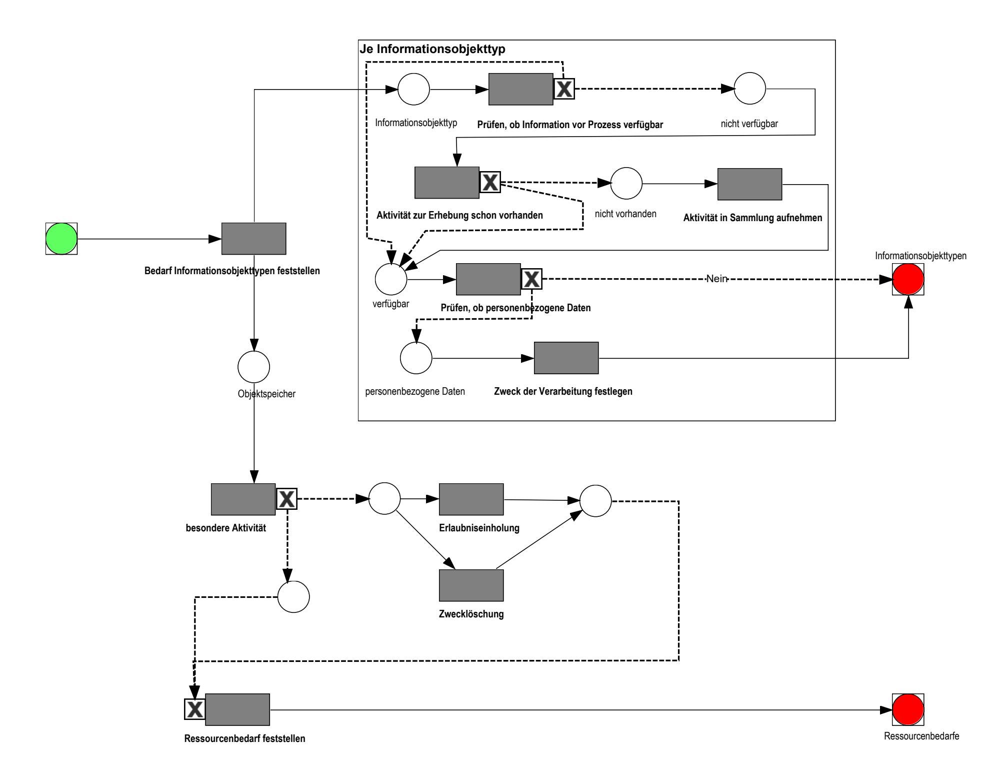


Abbildung 23: Verfeinerung der Aktivität „Aktivität beschreiben"

Die Aktivität „Aktivität beschreiben" ist auch entsprechend mit einem Kasten gekennzeichnet und in Abbildung 23 detaillierter modelliert. Die Modellierung zeigt auch, dass zur Definition einer Methode nicht nur die Definition der einzelnen Aktivitäten, sondern auch deren Ordnung innerhalb eines Vorgehensmodells und zugleich die Beschreibung der logischen Abhängigkeiten unter den Aktivitäten notwendig ist.

Betrachtet man die geordneten Aktivitäten, fällt zunächst auf, dass – abweichend vom üblichen skizzierten Lebenszyklus eines Geschäftsprozesses zwischen „Design und Modellierung" und „Einführung" – zunächst zwingend eine Phase „Simulation und Auswertung" notwendig ist und – abhängig von deren Ergebnis – wieder zurück zur Analyse gesprungen werden muss. In Abbildung 24 ist die neue Phase „Simulation und Auswertung" blau hervorgehoben und der mögliche Rücksprung orangefarben

belegt. Dieses Vorgehen ist nicht prinzipiell neu. Auch wenn es in den von de Morais u. a. (de Morais u. a., 2014) analysierten Lebenszyklen in keinem grafisch skizziert ist: Es war auch bisher üblich, in irgendeiner Form die Qualität des Geschäftsprozesses vor seiner Einführung zu bewerten. In dieser Arbeit wird diese Phase aber dennoch besonders hervorgehoben, weil einige Aspekte, wie beispielsweise die Datenminimierung von personenbezogenen Daten, erst mithilfe dieser Phase betrachtet werden.

Zur PriCon4BPM-Methode gehören insbesondere die nachfolgenden **Artefakte:**

- Sammlung der Aktivitäten. Hierzu ist keine spezifische Sprache vorgesehen, da die Aktivitäten und die zusätzlich dazu gesammelten Informationen (wie beispielsweise Zweck) später als Informationsvertraulichkeits- und Datenschutz-Netz formalisiert werden.
- Informationsobjekttypen wie Objekttypen und Ressourcen, wie beispielsweise im Horus Business Modeler vorgesehen, sodass eine Verknüpfung mit dem Geschäftsprozess möglich ist.
- Simulationsprotokoll in der Sprache (hier ein XML-Format), wie in Kapitel 6.4 spezifiziert.
- Simulations- und Analyseauswertung hinsichtlich Einhaltung von Informationsvertraulichkeit, Zweckbindung und Datenminimierung.
- Modell des Prozesses in der definierten Sprache des Informationsvertraulichkeits- und Datenschutz-Netzes, wie in Kapitel 5.3 spezifiziert.

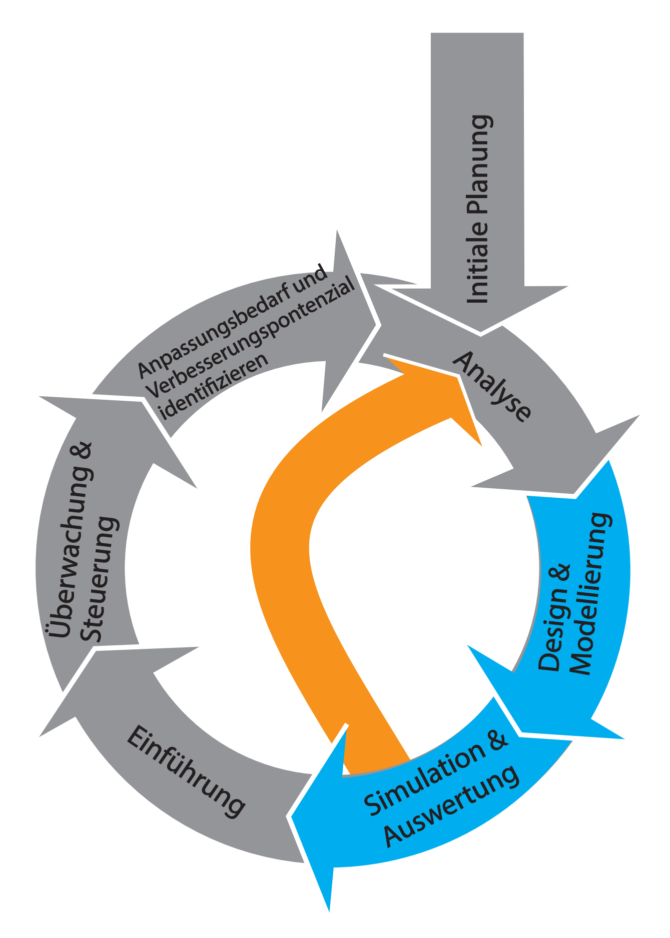


Abbildung 24: angepasster Lebenszyklus des Geschäftsprozessmanagements

Insbesondere die beiden geschaffenen Sprachen Informationsvertraulichkeits- und Datenschutz-Netze (ICPN, Kapitel 5.3) und ICPN-Trace (Kapitel 6.4) präzisieren die Anwendung der gesamten Methode und sind somit wesentlicher Bestandteil von PriCon4BPM. Durch die damit vorgegebene Syntax und Semantik wird das gemeinsame Verständnis der entsprechenden Artefakte wesentlich gefördert. Damit wird die Anwendbarkeit der PriCon4BPM-Methode unterstützt. Ihr fehlt jedoch noch eine vollständige **Werkzeugunterstützung**. Hierzu kommt später die Integration in den Horus Business Modeler in Betracht. Entweder muss das Werkzeug die Methode vollständig unterstützen, oder es muss andere Dienste integrieren beziehungsweise mit

ihnen kompatibel sein, um eine vollständige Unterstützung zu ermöglichen. Hierzu bietet sich die Verwendung von Microservices wie bei Alpers u. a. (Alpers, Becker, Oberweis & Schuster, 2015) an. Um hierfür ein Simulationswerkzeug bereitzustellen, wurde eine Java-basierte Webserviceschnittstelle für das in Prolog entwickelte PASIPP-Werkzeug (Oberweis, Seib & Lausen, 1991) geschaffen[1]. Es gibt also unterschiedliche Strategien, später eine Werkzeugunterstützung für PriCon4BPM bereitzustellen.

7.3 Anwendungsbeispiel

Die PriCon4BPM-Methode wird nachfolgend durch ein Anwendungsbeispiel weiter beschrieben. Als Beispiel dient der Bestell- und Bezahlprozess, den ein Neukunde für ein Produkt ausführt. Das Produkt ist in diesem Beispiel ein für den Kunden individuell bedrucktes Kleidungsstück. Zunächst gilt es, das Ziel des Geschäftsprozesses festzulegen: die Auslieferung des Artikels an den Kunden und die Bezahlung des Kaufpreises durch denselben. Anschließend sind die Aktivitäten zu sammeln. Für das Anwendungsbeispiel gehen wir davon aus, dass das Produkt bereits in einem Webshop ausgesucht wurde und verzichten auf die Modellierung von Ausnahmen (Fehler bei der Bezahlung etc.). Beim Sammeln der Aktivitäten kommt es noch nicht auf deren Reihenfolge an. Zu einigen Aktivitäten wurden Detailaktivitäten (zur Verfeinerung) gesammelt, für andere Aktivitäten wurde an dieser Stelle bewusst darauf verzichtet (die Verfeinerung soll hier nicht betrachtet werden).

- Erzeugen eines neuen leeren Designs
- Hochladen der Druckdaten (Bilddateien)
- Anordnen der Druckdaten
- Speichern und Freigeben des Designs
- Einwilligung zur Speicherung und Verarbeitung der Druckdaten

[1] Masterarbeit von Fabian Stolz am Karlsruher Institut für Technologie: „Integration von Prolog-Modulen in eine Microservice-Architektur“ (2018). Betreut von Sascha Alpers und Andreas Oberweis.

- Eingabe von Größe und Stückzahl
- Anlegen eines Kundenkontos
    - E-Mail-Adresse eingeben
    - Bestätigungs-E-Mail zusenden
    - Bestätigungs-E-Mail-Link klicken
    - Konto eröffnen und Passwort vergeben
    - Vorname, Name, Geburtsdatum und Postadresse eintragen
- Bezahlen per SEPA-Lastschrift
- Bezahlen per Rechnung
    - Bonitätsprüfung
    - Rechnungsversand
- Generieren der Druckdateien
- Überprüfung des Motivs bezüglich Unternehmensrichtlinien des Herstellers
- Bedrucken des Textils
- Versand des Textils

Anschließend werden je Aktivität weitere Informationen gesammelt beziehungsweise festgelegt. Dazu wird ein entsprechendes Formular verwendet, welches nun zunächst vorgestellt wird:

Aktivität	Name der Aktivität
notwendige Informationsobjekttypen	Hier werden alle Informationsobjekttypen aufgelistet, welche für die Aktivität notwendig sind. Dabei bedeutet „–“, dass keine Informationsobjekttypen zur Durchführung der Aktivität notwendig sind.
erzeugte Informationsobjekttypen	Hier werden alle Informationsobjekttypen aufgelistet, welche durch die Aktivität erzeugt werden. Dabei bedeutet „–“, dass keine Informationsobjekttypen erzeugt werden.

falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	Das Zeichen „–“ bedeutet hier, dass keine Informationsobjekttypen mit personenbezogenen Daten verwendet werden. Sonst werden hier je Informationsobjekttyp der Zweck bzw. die Zwecke der Verarbeitung gelistet. Hierzu wird zunächst der Informationsobjekttyp genannt, hinter einem Doppelpunkt folgt dann die Zweckangabe.
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Einige Aktivitäten erfüllen bestimmte Aufgaben hinsichtlich des Datenschutzes. Hierzu gehören Aktivitäten, durch welche die betroffene Person eine Einwilligung in einen bestimmten Verarbeitungszweck erteilt (bzw. diese Einwilligung widerruft). Ein anderes Beispiel ist die Schaffung eines Vertrages, für welchen die Verarbeitung erforderlich ist. „Nein“ bedeutet, dass es sich um keine solche Aktivität handelt. Bei „Ja“ erfolgt jeweils eine kurze Konkretisierung.
beteiligte Ressourcen	Hier werden die an der Aktivität beteiligten Ressourcen (Menschen und Systeme) aufgelistet.

Nachfolgend für die Aktivitäten des Anwendungsbeispiels die detaillierten und strukturierten Beschreibungen:

Aktivität	Erzeugen eines neuen leeren Designs
notwendige Informationsobjekttypen	–
erzeugte Informationsobjekttypen	• Design
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	–
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Designserver (Web)

Aktivität	Hochladen der Druckdaten
notwendige Informationsobjekttypen	• Design • Kundendatensatz
erzeugte Informationsobjekttypen	• Design-Bilddatei
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Kundendatensatz: Vertragserfüllung • Design: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Kunde • Designserver (Web)

Aktivität	Anordnen der Druckdaten
notwendige Informationsobjekte	• Design • Kundendatensatz • Design-Bilddatei
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Design-Bilddatei: Gestaltung • Kundendatensatz: Vertragserfüllung • Design: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Kunde • Designserver (Web)

Aktivität	Speichern und Freigeben des Designs
notwendige Informationsobjekte	• Design • Kundendatensatz • Design-Bilddatei
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Design-Bilddatei: Gestaltung • Kundendatensatz: Vertragserfüllung • Design: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Kunde • Designserver (Web)

Aktivität	Eingabe von Größe und Stückzahl
notwendige Informationsobjekttypen	• Kundendatensatz • Design • Design-Bilddatei
erzeugte Informationsobjekttypen	Bestellung
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Kundendatensatz: Vertragserfüllung • Design-Bilddatei: Gestaltung • Design: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Kunde • CRM-Server

Aktivität	E-Mail-Adresse eingeben
notwendige Informationsobjekttypen	–
erzeugte Informationsobjekttypen	• E-Mail-Adresse
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	–
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Ja, Erlaubnistatbestand Vertragserfüllung
beteiligte Ressourcen	• Kunde • CRM-Server

Aktivität	Bestätigungs-E-Mail zusenden
notwendige Informationsobjekte	• E-Mail-Adresse
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• E-Mail-Adresse: Vertragserfüllung (inkl. vorvertragliche Maßnahmen)
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server

Aktivität	Bestätigungs-E-Mail-Link klicken
notwendige Informationsobjekttypen	• E-Mail-Adresse
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• E-Mail-Adresse: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server

Aktivität	Konto eröffnen und Passwort vergeben
notwendige Informationsobjekttypen	• E-Mail-Adresse
erzeugte Informationsobjekttypen	• Kundendatensatz
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• E-Mail-Adresse: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Ja, Erlaubnistatbestand Vertragserfüllung
beteiligte Ressourcen	• CRM-Server

Aktivität	Vorname, Name, Geburtsdatum und Postadresse eingeben
notwendige Informationsobjekttypen	• Kundendatensatz
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Kundendatensatz: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server

Aktivität	Bezahlen per SEPA-Lastschrift
notwendige Informationsobjekttypen	• Bestellung • Kundendatensatz
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Bestellung: Vertragserfüllung • Kundendatensatz: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server • SEPA-Einzugsdienstleister

Aktivität	Kundenwunsch „Bezahlen per Rechnung"
notwendige Informationsobjekttypen	• Bestellung • Kundendatensatz
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Bestellung: Vertragserfüllung • Kundendatensatz: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Ja, in Bonitätsprüfung einwilligen
beteiligte Ressourcen	• CRM-Server

Aktivität	Bonitätsprüfung
notwendige Informationsobjekttypen	• Bestellung • Kundendatensatz
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieses Informationsobjekttypen	• Bestellung: Bonitätsprüfung • Kundendatensatz: Bonitätsprüfung
spezielle Datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server • Dienstleister Bonitätsprüfung

Aktivität	Rechnungsversand
notwendige Informationsobjekttypen	• Bestellung • Kundendatensatz
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieses Informationsobjekttypen	• Bestellung: Bonitätsprüfung • Kundendatensatz: Bonitätsprüfung
spezielle Datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server • Forderungssystem

Aktivität	Generieren der Druckdaten
notwendige Informationsobjekttypen	• Bestellung • Kundendatensatz • Design • Design-Bilddatei • Schnittmuster Textil
erzeugte Informationsobjekttypen	• Druckdaten
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Bestellung: Vertragserfüllung • Kundendatensatz: Vertragserfüllung • Design: Gestaltung • Design-Bilddatei: Gestaltung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Designserver (Web)

Aktivität	Überprüfung des Motivs bezüglich Unternehmensrichtlinien des Herstellers
notwendige Informationsobjekttypen	• Design-Bilddatei • Unternehmensrichtlinien des Herstellers
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieses Informationsobjekttypen	• Design-Bilddatei: Motivprüfung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server • Motivprüfer

Aktivität	Bedrucken des Textils
notwendige Informationsobjekttypen	• Druckdaten • Bestellung
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	Druckdaten: Vertragserfüllung Bestellung: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• Produktionsserver • Produktionsmitarbeiter • Druckmaschine

Aktivität	Versand des Textils
notwendige Informationsobjekttypen	• Kundendatensatz • Bestellung
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieses Informationsobjekttypen	• Bestellung: Vertragserfüllung • Kundendatensatz: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	Nein
beteiligte Ressourcen	• CRM-Server • Versandmitarbeiter • Versanddienstleister

Je Informationsobjekttyp werden anschließend für die spätere Modellierung weitere Informationen strukturiert erfasst.

Informationsobjekttyp	Design
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja (das Design ist über die Bestellung während der Bearbeitung mit dem Besteller verknüpft)
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	Kundendatensatz
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	Design-Bilddatei
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	E-Mail-Adresse
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	Bestellung
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	Druckdaten
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	Geburtsdatum
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Nein
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	Ja
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Ja
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Informationsobjekttyp	Schnittmuster Textil
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Ja
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja“ setzen.)	– (nicht relevant, weil die Informationen bereits vorher vorliegen)
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Nein
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Ja – das Schnittmuster der einzelnen Textilien ist ein Geschäftsgeheimnis (vergleichbar mit den Leisten des Schusters)

Die Informationen zu Schnittmuster Textil müssen also geschützt werden. Daher wird für den Zugriff auf diesen Informationsobjekttyp die Zuordnung zur Rolle „internes System“ gefordert.

Informationsobjekttyp	Unternehmensrichtlinien des Herstellers
Liegen die Informationen bereits vor Ausführung des Geschäftsprozesses vor?	Ja
Falls die Informationen nicht bereits vor Ausführung des Geschäftsprozesses vorliegen: Gibt es eine Aktivität, um diese zu sammeln? (Falls nein: Aktivität hinzufügen und danach Wert auf „ja" setzen.)	– (nicht relevant, weil die Informationen bereits vorher vorliegen)
Sind personenbezogene Daten enthalten? (Ggf. Begründung zur späteren Nachvollziehbarkeit ergänzen.)	Nein
Ist der Informationsobjekttyp schützenswert im Sinne von Betriebs- und Geschäftsgeheimnissen?	Nein

Analog sind die beteiligten Ressourcen aus den Aktionen zu extrahieren und deren Rollenzuordnung hinsichtlich der Informationsvertraulichkeit festzulegen:

Ressource	Rollen
Designserver (Web)	IT-Web verfügbar
Kunde	Kunde
CRM-Server	IT-Web verfügbar
SEPA-Einzugsdienstleister	Finanzdienstleister
Dienstleister Bonitätsprüfung	Finanzdienstleister
Forderungssystem	internes System
Motivprüfer	Mitarbeiter
Produktionsserver	internes System
Produktionsmitarbeiter	Mitarbeiter
Druckmaschine	Produktionsressource
Versandmitarbeiter	Mitarbeiter
Versanddienstleister	Logistikdienstleister

Anschließend sind die Aktivitäten zu ordnen (hier ohne Darstellung), bevor ihre Modellierung als Informationsvertraulichkeits- und Datenschutz-Netz erfolgt. Für die

folgenden Modelle wird hierzu der Horus Business Modeler verwendet; daher werden zunächst die Informationsobjekttypen in Horus erfasst. Das Ergebnis ist in Abbildung 25 dargestellt. Ebenfalls ist das Ressourcenmodell zu übertragen. Danach kann das Informationsvertraulichkeits- und Datenschutz-Netz grafisch beschrieben werden.

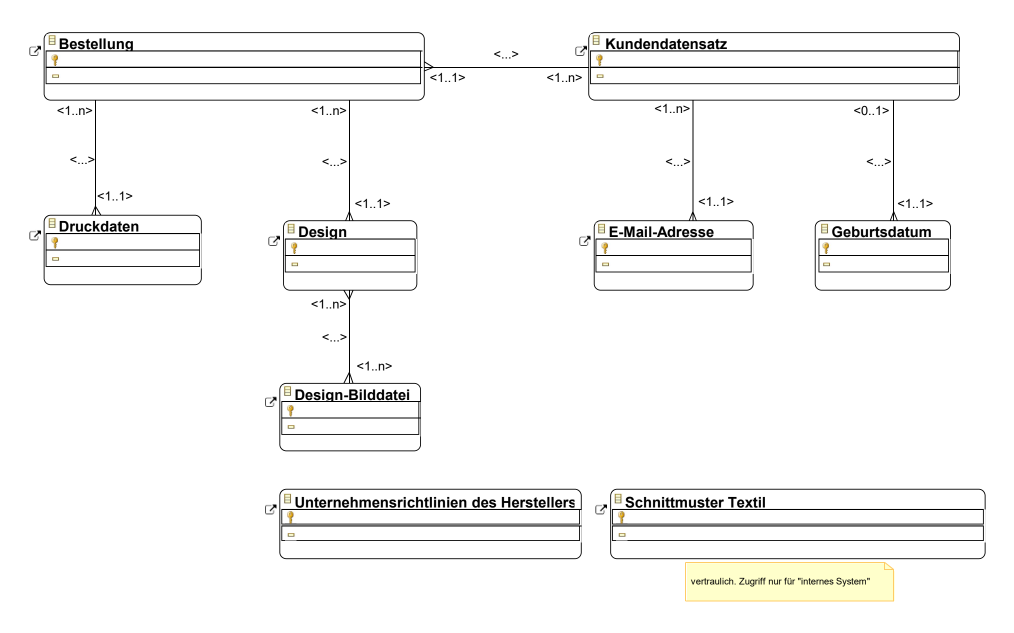


Abbildung 25: Informationsobjekttypmodell zum Anwendungsbeispiel; modelliert mittels Horus.

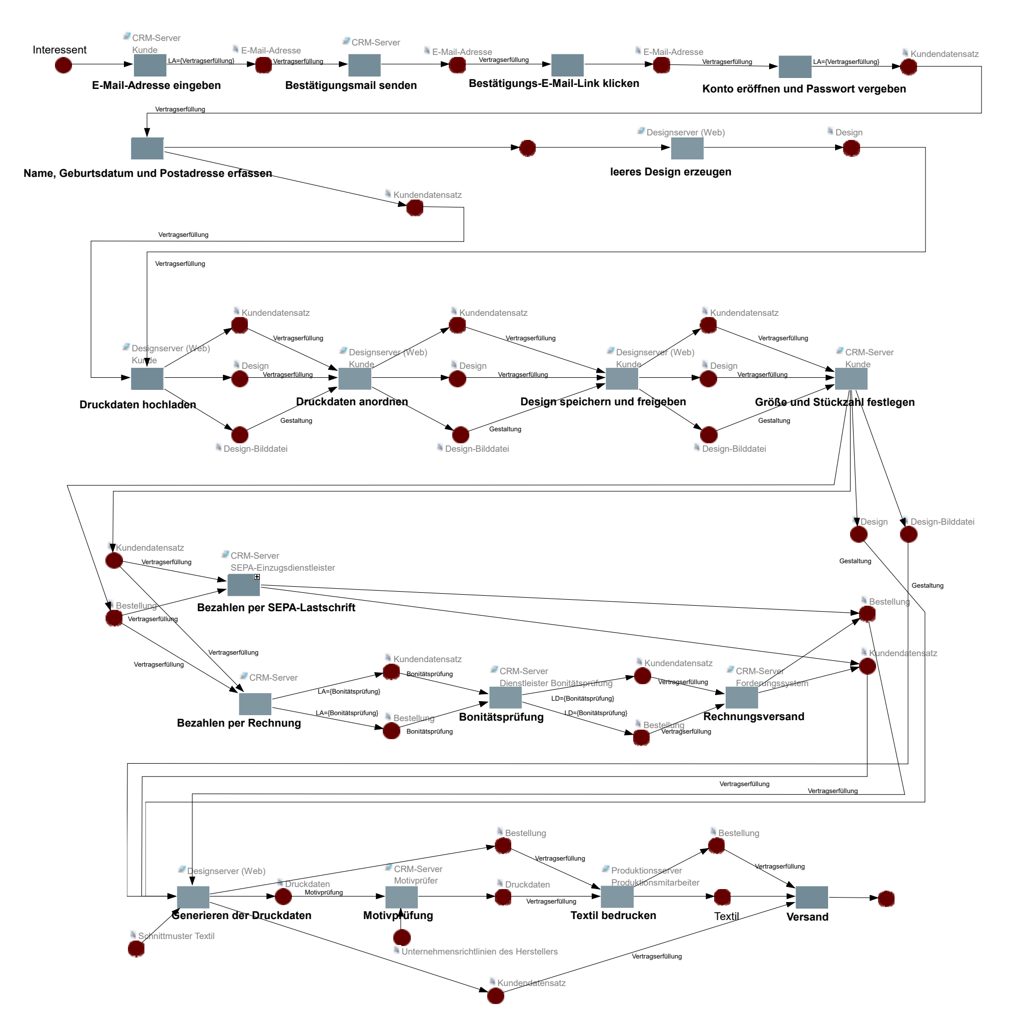


Abbildung 26: Bestellprozess als Informations- und Vertraulichkeits-Netz

Die Simulation und ihre Auswertung des Informationsvertraulichkeits- und Datenschutz-Netzes zeigen jedoch, dass der Prozess so noch nicht eingeführt werden kann. Folgende Probleme können in mehreren Zyklen erkannt werden:

- Der Prozess blockiert vor der Transition „Generierung der Druckdaten“. Der Grund ist, dass die Ressource nicht zur Rolle „internes System“ gehört und daher die Informationsvertraulichkeit des Schnittmusters verletzt würde.
- Außerdem zeigt eine genauere Betrachtung der Datenminimierung, dass das Geburtsdatum im Kundendatensatz nur für die Bonitätsprüfung im Falle der Rechnungszahlung benötigt wird.

Der Prozess muss zurück in die erste Lebenszyklusphase („Analyse“) des Geschäftsprozessmanagements (Abbildung 24), bis die Probleme gelöst werden. Der Prozessdesigner kann mithilfe der Erkenntnisse aus der Simulationsauswertung überprüfen, wie der Prozess oder die Ressource so geändert werden kann, dass die Forderung eingehalten wird. Hier werden folgende Verbesserungen vorgenommen:

- Der Prozessschritt wird von einer anderen Ressource (hier der Produktionsserver), die bereits über die entsprechende Rolle „internes System“ verfügt, ausgeführt. So kann die Vertraulichkeit des Schnittmusters durch die Anforderung „internes System“ weiter gewährleistet werden.
- Außerdem wird das Geburtsdatum im veränderten Prozess nur im Falle einer Bonitätsprüfung unmittelbar zuvor erfasst.
- Es wird in der Aktivität „Hochladen der Druckdaten“ eine Einwilligung für den Zweck „Gestaltung“ und eine für den Zweck „Motivprüfung“ eingeholt.

Die hinzugekommenen Aktivitäten sind:

Aktivität	Einwilligung Speichern und Verarbeiten der Druckdaten
notwendige Informationsobjekttypen	Kundendatensatz
erzeugte Informationsobjekttypen	–
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	• Kundendatensatz: Protokollierung Einwilligung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	ja
beteiligte Ressourcen	• Kunde • CRM-Server

Aktivität	Geburtsdatum eingeben
notwendige Informationsobjekttypen	Kundendatensatz
erzeugte Informationsobjekttypen	Geburtsdatum
falls Informationsobjekttypen personenbezogene Daten enthalten (siehe entsprechende Tabellen) – Festlegen des Zweckes der Verarbeitung dieser Informationsobjekttypen	Kundendatensatz: Vertragserfüllung
spezielle datenschutzrechtliche Aktivität (beispielsweise Einwilligung, Widerruf)	nein
beteiligte Ressourcen	• CRM-Server

Der umgestaltete Prozess ist dann erneut zu analysieren. In diesem Fall gibt es keine weiteren Schwierigkeiten, sodass der Prozess eingeführt werden kann.

8 Einordnung der PriCon4BPM-Methode

In diesem Kapitel werden zunächst Anforderungen an den Umgang mit Informationsvertraulichkeit und Datenschutz in Unternehmen auf der Ebene des Geschäftsprozessdesigns und Geschäftsprozessmanagements betrachtet und anschließend der eigene Ansatz sowie existierende Ansätze verwendeter Arbeiten mit diesen Anforderungen verglichen. Im Anschluss wird mithilfe des exemplarischen Einsatzes der PriCon4BPM-Methode durch unterschiedliche Personen in unterschiedlichen Szenarien ein erster Indikator für die Anwendbarkeit der Methode beschrieben und ausgewertet.

8.1 Anforderungen

Um Informationsvertraulichkeit und Datenschutz in Unternehmen auf der Ebene des Geschäftsprozessdesigns und Geschäftsprozessmanagements in geeigneter Weise zu unterstützen, sind verschiedene – teilweise bereits eingeführte – Anforderungen (A1 bis A10) relevant:

- A1: Methodische Unterstützung für das Design von Geschäftsprozessen Das Design von Geschäftsprozessen gestaltet sich für Fachanwender bereits ohne die systematische Betrachtung von Informationsvertraulichkeits- und Datenschutz-Aspekten als herausfordernd. Durch die genannten zusätzlichen Aspekte nimmt die Komplexität weiter zu; somit steigt auch die Bedeutung einer methodischen Unterstützung.
- A2: Informationsvertraulichkeit
    - A2a: Möglichkeit, die Vertraulichkeitsgrade verschiedener Informationsobjekttypen zu unterscheiden. Nicht alle Informationen in einer Organisation sind vertraulich, und auch die vertraulichen

  Informationen bedürfen nicht alle des gleichen Schutzes. Um eine sinnvolle, das heißt auch ökonomische, Prozessgestaltung zu ermöglichen, ist die Unterscheidung verschiedener Klassen der Informationsvertraulichkeit notwendig.
  - A2b: Eine klassenbasierte Informationsvertraulichkeit (A2a) ist notwendig, aber nicht hinreichend, um typische Sachverhalte abzubilden. Insbesondere, um den Kreis der Ressourcen, welche eine Information zur Kenntnis nehmen beziehungsweise verarbeiten darf, weiter zu beschränken, ist querliegend ein zusätzliches Kriterium erforderlich. Damit sollen neben der klassenbasierten Vertraulichkeit aufgabenbezogene Vertraulichkeitsregeln durchgesetzt werden. Eine Möglichkeit hierfür ist ein Rollenmodell.
  - A2c: Ob eine Ressource eine bestimmte Information zur Kenntnis nehmen darf, kann auch davon abhängen, welche Informationen ihr bereits bekannt sind. Mit der Berücksichtigung bereits bekannter Informationen kann verhindert werden, dass durch die Kombination vieler einzelner nicht vertraulicher Informationen letztendlich doch eine vertrauliche Information gewonnen werden kann.
  - A2d: Ob eine Aktion durch eine Ressource ausgeführt werden darf, kann davon abhängen, welche Informationen die Ressource schon kennt. So kann beispielsweise verhindert werden, dass eine Information aus einem Beratungsprojekt mit Kunde A in ein Projekt mit Kunde B einfließt (Umsetzung des Chinese-Wall-Prinzips).
- A3: Informationsobjekttypen
  - A3a: Möglichkeit, Informationsobjekttypen im Geschäftsprozess zu berücksichtigen
- Wenn Informationsvertraulichkeit untersucht werden soll, ist es zielführend, auch die Betrachtung von Informationsobjekttypen zu ermöglichen.

Dabei können Informationsobjekttypen im Prozess verarbeitet werden, das heißt Input für eine Aktivität sein und/oder Ergebnis einer Aktivität sein.

  - A3b: Möglichkeit, auf die Veränderung gespeicherter Informationen (beispielsweise durch Entfernen sensibler Daten, Verschlüsselung oder Anonymisierung) mit einer Aktivität durch Änderung der Vertraulichkeit beziehungsweise der Berechtigungen zu reagieren

- A4: Möglichkeit, Ressourcen im Geschäftsprozess zu berücksichtigen Letztlich werden die Aktivitäten eines Geschäftsprozesses mithilfe von Ressourcen erbracht. Da Letztere ggf. auch die verarbeiteten Informationen erhalten, ist es zielführend, ihre Mitwirkung im Prozess systematisch betrachten zu können.
- A5: Möglichkeit, den Kontrollfluss im Geschäftsprozess unabhängig aber auch mit integriertem Datenfluss abbilden zu können.
- A6: Die Modellierung muss die Kontrolle darüber ermöglichen, inwieweit ein Geschäftsprozess die Verarbeitungsgrundsätze der EU-DS-GVO beachtet. Die Verarbeitungsgrundsätze sind:
  - A6a: Rechtmäßigkeit
  - A6b: Verarbeitung nach Treu und Glauben
  - A6c: Transparenz
  - A6d: Zweckbindung
  - A6e: Datenminimierung
  - A6f: Richtigkeit
  - A6g: Speicherbegrenzung
  - A6h: Integrität und Vertraulichkeit
  - A6i: Rechenschaftspflicht
- A7: Darüber hinaus ist es wünschenswert, den Modellierer nicht nur bei der Darstellung von erarbeiteten Regeln zu unterstützen, sondern ihm auch bereits Hilfe zu bieten, wenn es um die Erarbeitung dieser Regeln geht.
- A8: Aufdeckung missbräuchlicher Verwendung

- Lässt sich leicht erkennen, ob die Methode missbräuchlich verwendet wurde, um beispielsweise möglichst viele Daten zu erheben und die entsprechenden Rechtfertigungsgründe zu finden?
- A9: Analyse und/oder Simulation
- Bei komplexen Prozessen, oder wenn es eine Vielzahl von Prozessen zu betrachten gilt, ist es nicht praktikabel, alle Fragen dadurch zuverlässig zu beantworten, dass der Modellierer über die Kompetenz verfügt, Eigenschaften zu den modellierten Prozessen zu erheben. Daher ist eine Analyseunterstützung beispielsweise durch eine Simulation und deren Auswertung notwendig.
- A10: Unterstützung bei der Implementierung des Prozesses – beispielsweise Transformation in BPEL oder Hilfe bei der Ableitung von Anforderungen an (Individual-) Softwaresysteme (beispielsweise durch entsprechende Modelle in UML)

8.2 Eigene und verwandte Arbeiten

Die Herausforderungen „Sicherheit" beziehungsweise „Datenschutz" in Geschäftsprozessen werden auch von anderen Ansätzen in unterschiedlicher Art und Weise adressiert. Diese Ansätze werden bei Alpers u. a. (Alpers u. a., 2018) und bei Alpers u. a. (Alpers, Pilipchuk, Oberweis & Reussner, 2019) identifiziert und vorgestellt[1]. Nachfolgend werden sie mit den dargestellten Anforderungen verglichen. In der letzten Spalte der Tabelle 6 wird zudem die PriCon4BPM-Methode mit den Anforderungen verglichen.

[1] Beide Veröffentlichungen untersuchen existierende Literatur hinsichtlich vorhandener Ansätze primär zur Betrachtung von Datenschutz (aber auch zu IT-Sicherheit) in Geschäftsprozessen und bei der Implementierung von Unternehmenssoftware. Hier werden nur die für Geschäftsprozesse relevanten Ansätze weiter analysiert.

Tabelle 6: Vergleich verschiedener Ansätze hinsichtlich der Anforderungen (+ wird unterstützt; - wird nicht unterstützt)

	(Accorsi & Wonnemann, 2011)	(Atluri & Huang, 2000)	(Knorr, 2001)	PriCon4BPM
A1: methodische Unterstützung	-	-	-	+
A2a: klassenbasierte Informations-vertraulichkeit	+	+	+	+
A2b: rollenbasierte Informationsvertraulichkeit	+	+	-	+
A2c: Aggregation von Informationsobjekttypen	-	-	-	+
A2d: prozessinstanz-übergreifende Kenntnisnahme von Informationen	-	+	-	-
A3a: Informationsobjekttypen mit Geschäftsprozess verknüpfen	-	-	-	+
A3b: Anpassung der Informationsvertraulichkeit	-	-	-	+
A4: Ressourcenverknüpfung	-	-	-	+
A5: Kontrollfluss	-	-	-	+
A6a: Rechtmäßigkeit	-	-	-	+
A6b: Verarbeitung nach Treu und Glauben	-	-	-	-
A6c: Transparenz	-	-	-	-
A6d: Zweckbindung	-	-	-	+
A6e: Datenminimierung	-	-	-	+
A6f: Richtigkeit	-	-	-	-
A6g: Speicherbegrenzung	-	-	-	-
A6h: Integrität und Vertraulichkeit	-	-	+	+
A6i: Rechenschaftspflicht	-	-	-	+

A7: Unterstützung bei Regelerarbeitung	-	-	-	+
A8: missbräuchliche Verwendung	+	-	-	-
A9: Analyse	+	-	-	+
A10: Implementierungs-unterstützung	-	+	-	-[2]

Wie dargestellt, setzt PriCon4BPM mit der Sprache der Informationsvertraulichkeits- und Datenschutz-Netze nicht alle Anforderungen um – stellt aber bezogen auf diese Anforderungen einen offensichtlichen Mehrwert gegenüber den verwandten Arbeiten dar (diese haben teils hier nicht beschriebene Stärken für andere Anwendungsfälle, wie beispielsweise die Modellierung von technischen Prozessen).

8.3 Anwendbarkeit

Die Sprache der Informationsvertraulichkeits- und Datenschutz-Netze sowie die PriCon4BPM-Methode wurden in der Anwendung durch verschiedene studentische Hilfskräfte initial erprobt. Dazu wurden diverse Beispielprozesse aus dem Handel mit Endkunden (beispielsweise eines Onlineshops für Schuhe) herangezogen. Anhand der Verwendung realer Prozesse (soweit diese durch die Darstellung des Unternehmens beziehungsweise eines Beispielkaufes erhoben werden konnten) lässt sich auch die Verwendbarkeit in realen Szenarien betrachten. Bei der Auswahl der Beispiele wurde ebenfalls darauf geachtet, dass auch Prozesse vorkommen, welche unternehmensübergreifend ausgeführt werden. Ein solches Beispiel war etwa durch das System gaxsys[3] – einer Onlinehandelsplattform für den Einzelhandel – gegeben.

[2] Im Rahmen dieser Arbeit wurden keine Konzepte zur Transformation entwickelt. Jedoch ist diese grundsätzlich vorgesehen und wird – als Idee – bei Alpers u. a. (Alpers, Pilipchuk, Oberweis & Reussner, 2018) beschrieben.

[3] https://gaxsys.com/

In diesem Fall waren die Prozesse aufgrund einer studentischen Abschlussarbeit (Hemriti, 2011) bekannt.

Es konnte gezeigt werden, dass PriCon4BPM auch durch Dritte (aufgrund der hier verfügbaren Beschreibung) angewendet werden kann. Die Sammlung von Aktivitäten vor der genaueren Erhebung von Daten zur jeweiligen Aktivität und vor der Anordnung innerhalb des Ablaufmodells, wie sie die PriCon4BPM-Methode vorsieht, hat sich in diesen Anwendungsfällen bewährt.

Zudem wurden im Rahmen eines Forschungsprojekt-Workshops mit wissenschaftlichen Mitarbeitern zweier Forschungseinrichtungen sowie Mitarbeitern zweier Industriepartner einzelne Artefakte angewandt. Dabei wurden der Ablauf anhand eines bestehenden Prototyps aufgenommen und die verarbeiteten personenbezogenen Daten erfasst. Die verarbeiteten Daten wurden anschließend Zwecken zugewiesen, und es wurde jeweils ein Erlaubnistatbestand hierfür festgelegt. Eine Schwachstelle der Sicht der Geschäftsprozesse ist dabei aufgefallen, und dadurch wurde identifiziert, dass eine technische Sicht zu ergänzen ist. Konkret werden bei der Betrachtung der einzelnen Aktivitäten als benötigte Daten nur solche erfasst, die direkt dem Geschäftsprozess dienen, weil diese von den Geschäftsprozessdesignern so berichtet werden. Technische Daten, das heißt beispielsweise Verbindungsdaten wie eine IP-Adresse, die ggf. vom Webserver in Logs aufgezeichnet wird, wurden von Geschäftsprozessdesignern nicht genannt, aber später bei der technischen Konzeption erkannt. Dies ist als Grenze der PriCon4BPM-Methode zu verstehen.

9 Fazit und Ausblick

In diesem Kapitel wird zunächst ein Fazit zur Arbeit gezogen. Dazu werden die wesentlichen Ergebnisse der Arbeit zusammengefasst und eingeordnet. Das Fazit schließt mit der Betrachtung der Grenzen des Ansatzes. Anschließend wird ein Ausblick auf weiterführende Forschungsarbeiten gegeben.

9.1 Fazit

Bisherigen Ansätzen zur Betrachtung von Datenschutz und Informationsvertraulichkeit in Unternehmen fehlt es teilweise an einer dafür erweiterten Modellierungssprache und teilweise an der notwendigen allgemeinen Einsetzbarkeit aufgrund einer zu hohen Spezialisierung des Ansatzes. Ziel der vorliegenden Arbeit war es daher, sowohl Sicherheit als auch Datenschutz bereits ab dem Entwurf bzw. ab der Überarbeitung von bestehenden Geschäftsprozessmodellen systematisch zu unterstützen. Dazu wurde eine Beschränkung auf Informationsvertraulichkeit als Aspekt der Sicherheit und auf Zweckbindung und Datenminimierung als Aspekte des Datenschutzes vorgenommen. Das Konzept wurde jedoch so entwickelt, dass keine neue Speziallösung für diese „Nischen“ geschaffen wurde, sondern dass es um weitere Aspekte wie beispielsweise Integrität (als Aspekt von IT-Sicherheit) und Speicherbegrenzung (als Aspekt des Datenschutzes) erweitert werden kann.

Als Basis für diesen Ansatz wurden als Modellierungssprache Petri-Netze verwendet, da diese sich aufgrund ihrer Formalisierung für präzise Analysen eignen, ihre grafische Repräsentation gut verständlich ist und die Sprache weit verbreitet in Forschung und Praxis ist. So können die hier vorgestellten Erweiterungen bzgl. Sicherheit und Datenschutz ergänzend zu vielen bestehenden Möglichkeiten von Petri-Netzen verwendet werden. Aufgrund dieser Basis ist die Einsetzbarkeit in vielen Szenarien gegeben. Der vorgestellte Ansatz bedarf der Unterscheidbarkeit von

Informationsobjekten, und auch dafür bieten höhere Petri-Netze (gefärbte Petri-Netze) die entsprechende Grundlage.

Diese Grundlage wird von den im Rahmen dieser Dissertation entwickelten Informationsvertraulichkeits- und Datenschutz-Netzen zur Modellierung von Informationsvertraulichkeit, Zweckbindung und Datenminimierung erweitert. Hierzu genügt die Sicht der Geschäftsprozesse auf ein Unternehmen alleine nicht aus; der Ansatz integriert daher zusätzlich die Sicht der Datenstruktur und die Sicht der Organisationsstruktur. Die Verknüpfung verschiedener Sichten ist nicht vollständig neu, sie wird grundsätzlich auch bereits von sogenannten Modellierungssuiten unterstützt (zum Beispiel vom Horus Business Modeler). Dieses Prinzip wird hier aber für die neue, integrierende Modellsicht der Informationsvertraulichkeit und des Datenschutzes genutzt, und die Verbindung der entsprechenden, zugrunde liegenden Sichten wird formal definiert.

Die spezifizierten Modellierungsmöglichkeiten für die Informationsvertraulichkeit eignen sich für einen praktischen Einsatz der Methode. Informationen können klassifiziert werden, insbesondere lässt sich durch Zuordnung zu einer Klasse ausdrücken, dass eine Information besonders sensibel ist und der Zugang zu ihr entsprechend stark begrenzt sein muss. Dies kann kombiniert werden mit rollenbasierten Berechtigungen. Insbesondere kann bestimmt werden, dass eine Ressource eine bestimmte Rolle haben muss (oder mehrere), um eine Information erhalten zu dürfen. In der Kombination von beiden Restriktionen können viele Arten von Anforderungen modelliert werden. Dabei können auf der einen Seite sowohl statische Restriktionen bzgl. Informationsobjekttypen, d. h. für alle Informationsobjekte eines Typs, als auch dynamische Restriktionen (beispielsweise Veränderung der Informationsvertraulichkeit innerhalb eines Prozesses durch Änderung der Informationen im Informationsobjekt wie bei der Kürzung der Kreditkartennummer auf die letzten 4 Stellen) abgebildet werden. Auf der anderen Seite können personelle und maschinelle Ressourcen einzelnen informationsverarbeitenden Aktivitäten zugeordnet werden.

Dadurch lässt sich ausdrücken, welche Ressourcen ein Informationsobjekt während der Prozessausführung zur Kenntnis nehmen.

Bezüglich des Datenschutzes wurden für zwei von insgesamt neun von der EU-DS-GVO in Artikel 5 aufgeführten Grundsätze des Datenschutzes Spracherweiterungen entwickelt. Diese sind vollständig kompatibel zur Erweiterung für Informationsvertraulichkeit, sodass die insgesamt drei Erweiterungen (Informationsvertraulichkeit, Zweckbindung, Datenminimierung) nicht nur isoliert, sondern auch in beliebigen Kombinationen verwendet werden können. Für den Grundsatz der Zweckbindung wurde es ermöglicht, Informationsobjekte mit legitimierten Verarbeitungszwecken zu verknüpfen. Dabei wird die Verknüpfung durch den Prozess selbst vorgenommen, sodass beispielsweise nach Einholen einer Einwilligung für einen bestimmten Zweck dieser mit dem Informationsobjekt verknüpft werden kann. Neben dem Erlaubnistatbestand Einwilligung können aber natürlich auch Zwecke, die sich aus anderen Erlaubnistatbeständen ergeben, wie beispielsweise Verarbeitung aufgrund der Notwendigkeit zur Erfüllung eines Vertrages mit dem Betroffenen, verknüpft werden. Dabei ist es auch möglich, für wegfallende Zwecke (beispielsweise bei Widerruf der Einwilligung oder aufgrund ihrer Erledigung) die Verknüpfung wieder zu entfernen. Bei der Datenminimierung wird es im Rahmen der Modellierung ermöglicht, die Aktivitäten mit dem Bedarf an Daten zu verknüpfen. Die minimal notwendige Datenmenge für einen Prozess bzw. Pfad kann dann in der Analyse ermittelt werden.

Dadurch wurde die Möglichkeit neu geschaffen, sowohl Informationsvertraulichkeit als auch Datenschutz in Geschäftsprozessmodellen systematisch auszudrücken. Die Informationsvertraulichkeits- und Datenschutz-Netze ermöglichen es, dass Geschäftsprozessverantwortliche, Experten für Anforderungen der IT-Sicherheit und Experten für den Datenschutz gemeinsam – in einer für alle verständlichen und eindeutigen Sprache – einen Prozess definieren. Dies ist auch deshalb wichtig, weil verschiedene Personen die unterschiedlichen Aspekte verantworten und oft auch eine Governance-Funktion dafür ausüben.

Wenn Verantwortliche für mehrere Prozesse zuständig sind, reicht die eindeutige Darstellung durch Informationsvertraulichkeits- und Datenschutz-Netze alleine nicht aus. Sie müssen durch entsprechende Analyseregeln unterstützt werden. Dazu wurden Schaltbedingungen zur Ablaufvertraulichkeit und zur Zweckbindung entwickelt. In beiden Fällen ist es möglich, Informationsvertraulichkeits- und Datenschutz-Netze zunächst ohne die zusätzlichen Restriktionen der Schaltregeln zu simulieren und anschließend auszuwerten, welche Schaltfolgen aufgrund der neuen Restriktionen nicht mehr zulässig sind. Es ist ferner möglich zu analysieren, welche Ressourcen an einem Prozess beteiligt sein müssen (hinsichtlich ihrer Vertrauenswürdigkeitsklassen bzw. Rollenzugehörigkeiten), um einen Prozess ausführen zu können. Dadurch können die Auswirkungen der Restriktionen auf den Geschäftsprozess auch ökonomisch bewertet werden. Insbesondere, wenn verschiedene Prozessalternativen zur Erreichung eines Zieles zur Verfügung stehen, kann dieser Ansatz genutzt werden, um die für den jeweiligen Kontext passende Alternative auszuwählen. Insofern bietet dieser Ansatz den Verantwortlichen eine Entscheidungsunterstützung sowohl hinsichtlich der Verwendbarkeit von Geschäftsprozessen (sind diese regelkonform, d. h. compliant?) als auch bei der Bewertung verschiedener regelkonformer Alternativen. Hinsichtlich der Datenminimierung wurde ein anderer Weg gewählt. Hier ist keine Erweiterung der Schaltregel erforderlich, sondern es kann für jede Schaltfolge der Bedarf an Daten ermittelt werden – durch die Verknüpfung der Bedarfe mit den schaltenden Aktivitäten. Darauf aufbauend kann überprüft werden, ob nur benötigte Daten erhoben werden.

Zu den Zielen gehörte ferner, die Anwendung der neuen Informationsvertraulichkeits- und Datenschutz-Netze und ihrer Analysemöglichkeiten durch eine geeignete Methode zu unterstützen, bzw. aufbauend auf der Sprache und den Analysemöglichkeiten eine entsprechende Methode zu entwickeln. Daher wurde die PriCon4BPM-Methode als Anpassung existierender Konzepte zum Geschäftsprozessmanagement entwickelt. Durch das beschriebene planmäßige Vorgehen werden Modellierer und Verantwortliche angeleitet, die Möglichkeiten von Informationsvertraulichkeits- und

Datenschutznetzen für ganz unterschiedliche Geschäftsprozesse zu nutzen, um Informationsvertraulichkeit und Datenschutz umzusetzen bzw. weiter zu fördern. Die Methodenbeschreibung verdeutlicht auch, dass der Ansatz die Phasen „Design und Modellierung“ und „Simulation und Auswertung“ verändert und die vorangehende Analysephase erweitert. Die Implementierungsphase stand nicht im Fokus dieser Arbeit.

Eine Beschränkung des vorgestellten Ansatzes ist es, dass davon ausgegangen wird, dass die jeweiligen Verantwortungsträger bzw. Organisationen ein Interesse daran haben, Datenschutz und Informationsvertraulichkeit umzusetzen, und dass sie die Sprache und Methode nicht dazu nutzen wollen, um beispielsweise möglichst weitreichende Verarbeitungen personenbezogener Daten zu rechtfertigen. In letzterem Sinne geht der Ansatz von wohlwollenden Organisationen und Verantwortungsträgern aus.

Der Ansatz bietet keine Unterstützung bei der Bewertung spezifischer technischer Verfahren. Wenn beispielsweise eine Aktivität zur Anonymisierung von personenbezogenen Daten modelliert wird und im Folgenden die Eigenschaft, die angibt, ob es sich um ein personenbezogenes Datum handelt, auf „false“ gesetzt wird, dann kann der Ansatz keine geeigneten Verfahren oder Anonymisierungsmaßstäbe vorschlagen. Die Umsetzung der einzelnen Aktivitäten – und in dem Beispiel auch die Auswahl und richtige Parametrisierung eines entsprechenden Algorithmus – bleibt Aufgabe der jeweiligen Softwareentwicklung einschließlich der Auswahl eventueller Drittsysteme.

Der Ansatz betrachtet auch keine Wechselwirkungen zwischen verschiedenen Instanzen (Ausführungen) eines Prozesses. So kann mit dem Ansatz beispielsweise nicht direkt ausgedrückt werden, dass eine Information aus Prozessinstanz 1 zwar zur Kenntnis genommen werden darf, dass dann aber ein Mitwirken an Instanz 2 nicht möglich ist. Zwar könnte eine Ressource durch eine entsprechende Rolle auf eine bestimmte Instanz beschränkt werden, aber mangels dynamischer Rollenzuweisung zu Ressourcen kann dies noch nicht zur Laufzeit realisiert werden. Auch sind im

Ansatz aktuell keine Regeln vorgesehen, die eine Beteiligung ausschließen, wenn eine bestimmte Rolle zugewiesen ist.

Grenzen ergeben sich auch hinsichtlich der Bedrohungen. Betrachtet man die Bedrohungen aus Tabelle 1, so werden davon nur Offenlegung schützenswerter Informationen (G19, zum Beispiel aufgrund von Fahrlässigkeit), Verstoß gegen Gesetze oder Regelungen (G29), fehlerhafte Nutzung oder Administration von Geräten oder Systemen (G31, Wahrscheinlichkeit reduziert durch prozessbasierte, definierte Nutzung) und Missbrauch personenbezogener Daten (G38) durch den Ansatz direkt adressiert. Weitere auf Vertraulichkeit wirkende Bedrohungen wie beispielsweise das Abfangen kompromittierender Strahlung (G13) oder der Diebstahl von Geräten (G16) werden nicht adressiert. Auch daher kann der prozessbezogene Ansatz zur Umsetzung von Informationsvertraulichkeit nur ein Aspekt eines ganzheitlichen Sicherheitskonzeptes sein.

9.2 Ausblick

Die neu entwickelten Informationsvertraulichkeits- und Datenschutz-Netze können auch um weitere Aspekte des Datenschutzes ergänzt werden. Aufgrund der Konzeption der Sprache ist es möglich, dies durch kompatible zusätzliche Spracherweiterungen zu realisieren und anschließend die PriCon4BPM-Methode entsprechend anzupassen. Die konkrete Erweiterung ist abhängig vom jeweiligen Aspekt. Für das Beispiel der Rechtmäßigkeit wäre es ggf. zielführend, den Erlaubnistatbestand bzw. die Erlaubnistatbestände mit einem Prozessmodell bzw. den betreffenden Teilen zu verknüpfen und zu prüfen, ob das Ziel des Prozesses bzw. Subprozesses zum Erlaubnistatbestand passt. Bezüglich des Grundsatzes der Rechenschaftspflicht könnte untersucht werden, inwiefern durch die (ggf. erweiterten) Datenschutz-Netze die Informationspflicht nach Art. 5 Abs. 2 EU-DSG-VO erfüllt bzw. teilweise erfüllt werden kann. Es ist zu vermuten, dass ein entsprechend aufbereitetes Modell hier für die betroffenen Informationen dienlich sein kann.

Eine Aufgabe für weiterführende Arbeiten ist schließlich auch die komfortable Werkzeugunterstützung, um den praktischen Einsatz der Methode zu verbessern. Hier kann der Ansatz der mircoserviceorientierten Geschäftsprozessmodellierung und Analyse, wie er in Alpers u.a. (Alpers u. a., 2015) beschrieben ist, verwendet werden. Insbesondere Dienste für die Analyse von Informationsvertraulichkeits- und Datenschutz-Netzen können so umgesetzt und in verschiedene Editoren eingebunden werden. Hierzu wurde im Rahmen einer vom Autor der Arbeit betreuten Masterarbeit (Stolz, 2018) ein Ansatz erfolgreich getestet, welcher eine Analysekomponente für Petri-Netze bereitstellt[1], die auf der bis 1993 in der Programmiersprache Prolog am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) an der damaligen Universität Karlsruhe (TH) entwickelten Software PASIPP (Oberweis u. a., 1991) aufbaut. Auf PASIPP basierend kann ein Dienst weiterentwickelt und in das Prozessmodellierungswerkzeug Horus (aber auch in andere Modellierungssuiten) integriert werden.

Der Ansatz dieser Arbeit hilft dem Modellierer nicht dabei, Begriffe aus dem Datenschutzrecht wie personenbezogene Daten im jeweiligen Kontext korrekt auszulegen und anzuwenden. Dies ist schon deshalb schwierig, weil die Auslegung auch von Experten nicht für jeden Kontext einheitlich ist – insbesondere, wenn nicht die strengste (d. h. auch risikoaverseste) Auslegung angewendet werden soll, sondern eine zwar auch rechtskonforme, aber für einen Kontext besser passende Lösung gesucht wird. Hier kann das Informationsvertraulichkeits- und Datenschutz-Netz wie schon erörtert dazu verwendet werden, auch juristische Experten in die Diskussion einzubeziehen. In weiterführender Forschung ist zu prüfen, wie die Rechtsbegriffe durch ein Modell so beschrieben werden können, dass die Auslegung für Anwendungsfälle erleichtert werden kann. Am FZI Forschungszentrum Informatik läuft bereits ein entsprechendes Realisierungsvorhaben.

Der Ansatz ist dazu geeignet, das Vertrauen in Geschäftsprozesse zu fördern, bei denen diese von den jeweiligen Verantwortlichen wohlwollend und unter Einsatz von

[1] https://github.com/fzi-forschungszentrum-informatik/PasippMicroservice

Verstand und Empathie[2] zu den von der Datenverarbeitung bzw. Geschäftsprozessausführung Betroffenen entworfen werden. Allerdings wird nicht überwacht, ob der Prozess, wie er entworfen wurde, auch implementiert wird. Hierzu könnten aufgezeichnete Prozesslogs mit dem spezifizierten Prozess verglichen werden, um einen generellen Implementierungsfehler (d. h. die Abweichung von vielen Ausführungsinstanzen) aufzudecken (vgl. Mauser & Eggendorfer, 2017; Accorsi, Ullrich & van der Aalst, 2012). Dazu muss der Verstoß gegen das Prozessdesign aber bereits eingetreten sein, was evtl. bereits Schaden verursacht hat. Ein anderer Ansatz besteht darin, die korrekte Implementierung zu fördern. Dies kann von der Erhöhung des Modellverständnisses für Softwareentwickler durch Schulungen oder durch Transformation in eine ihnen geläufige Modellierungssprache wie UML geschehen. Ausgehend von dem UML-Modell könnten aber auch Ansätze modellgetriebener Softwareentwicklung weiterverfolgt werden (Alpers u. a., 2018). Dies würde auch das Vertrauen in die korrekte Implementierung – sowohl bei den Verantwortlichen als auch bei den Nutzern – fördern.

Die fehlerfreie Definition von Geschäftsprozessen ist besonders wichtig, da bei einer unzutreffenden Definition eine Vielzahl von Instanzen fehlerhaft durchgeführt wird. Wenn die Geschäftsprozessdefinition Regeln der IT-Sicherheit und des Datenschutzes fehlerhaft abbildet, wird also eine Vielzahl von Instanzen regelwidrig durchgeführt. Wenn Geschäftsprozesse automatisiert durchgeführt werden, sinkt zudem die Wahrscheinlichkeit, dass ein prozessbeteiligter Mensch den Fehler entdeckt und entsprechend reagieren kann. Durch die zunehmend automatisierte Ausführung von Geschäftsprozessen aufgrund verschiedener Entwicklungen wie dem zunehmenden Einsatz prozessgetriebener Unternehmenssoftware oder der automatisierten Bedienung vorhandener Unternehmenssoftware durch Softwareroboter (Aguirre & Rodriguez, 2017) wird die Bedeutung von Vertrauen in die korrekte Definition und Ausführung weiter zunehmen.

---

[2] Empathie der Verantwortlichen zu den Betroffenen ist notwendig, damit die Verantwortlichen sich für Lösungen entscheiden, welche die Rechte und Interessen der Betroffenen wahren.

10 Literaturverzeichnis

<kes> (2018). <kes>/Microsoft-Sicherheitstudie 2018 Lagebericht zur Sicherheit (3). In: <kes> Die Zeitschrift für Informations-Sicherheit, 34(6), S. 62–72.

Accorsi, R., Ullrich, M. & van der Aalst, W. M. (2012). Aktuelles Schlagwort: Process Mining. In: *Informatik Spektrum*, *35*(5), S. 354–359.

Accorsi, R. & Wonnemann, C. (2011). InDico: Information Flow Analysis of Business Processes for Confidentiality Requirements. In: *Security and Trust Management.* S. 194–209. Springer.

Aguirre, S. & Rodriguez, A. (2017). Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study. In: J. C. Figueroa-García, E. R. López-Santana, J. L. Villa-Ramírez & R. Ferro-Escobar (Hrsg.), *Applied Computer Sciences in Engineering*. S. 65–71. Springer.

Alpers, S., Becker, C., Oberweis, A. & Schuster, T. (2015). Microservice based tool support for business process modelling. In: A. Ghose & G. Grossmann (Hrsg.), *2015 IEEE 19th International Enterprise Distributed Object Computing Workshop*. S. 71–78. Adelaide.

Alpers, S., Eryilmaz, E., Hellfeld, S. & Oberweis, A. (2014). Mobile Modeling Tool based on the Horus Method. In: M. Boufaida & F. Kordon (Hrsg.), *International Workshop on Advanced Information Systems for Enterprises.* S. 65–71. Tunis: IEEE.

Alpers, S., Oberweis, A., Pieper, M., Betz, S., Fritsch, A., Schiefer, G. & Wagner, M. (2017). PRIVACY-AVARE: An approach to manage and distribute privacy settings. In: *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*. S. 1460–1468. Chengdu, China.

Alpers, S., Pieper, M. & Wagner, M. (2017). Herausforderungen bei der Entwicklung von Anwendungen zum Selbstdatenschutz. In: M. Eibl & M. Gaedke (Hrsg.), *Informatik 2017*. S. 1061–1072. Chemnitz: Gesellschaft für Informatik.

Alpers, S., Pilipchuk, R., Oberweis, A. & Reussner, R. (2018). Identifying Needs for a Holistic Modelling Approach to Privacy Aspects in Enterprise Software Systems. In: *4th International Conference on Information Systems Security and Privacy.* S. 74–82. Funchal, Madeira, Portugal.

Alpers, S., Pilipchuk, R., Oberweis, A. & Reussner, R. (2019). The Current State of the Holistic Privacy and Security Modelling Approach in Business Process and Software Architecture Modelling. In: P. Mori, S. Furnell & O. Camp (Hrsg.), *Information Systems Security and Privacy. Part of Communications in Computer and Information Science book series (volume 977).* S. 109-124. Springer.

Appl, C., Ekelhart, A., Fenz, N., Keiseberg, P., Leo, H., Kirrane, S., Polleres, A. Taudes, A., Treitl, V. & Singer, C. (2017). Big Data, Innovation und Datenschutz. Studie für eine DS-GVO kompatible Vorgangsweise zur Entwicklung einer Big Data Anwendung. Wien: Österreichisches Bundesministerium für Verkehr, Innovation und Technologie.

Atluri, V. & Huang, W.-K. (2000). A Petri Net Based Safety Analysis of Workflow Authorization Models. In: *Journal of Computer Security*, *8*(2), S. 209–240.

Avižienis, A., Laprie, J.-C. & Randell, B. (2004). Dependability and Its Threats: A Taxonomy. In: *Building the Information Society*. S. 91–120. Springer.

Baumann, U., Franz, E. & Pfitzmann, A. (2014). Sicherheit kryptographischer Systeme. In: *Kryptographische Systeme*. S. 63–105. Springer.

Bayerisches Landesamt für Datenschutzaufsicht (Hrsg.) (2018). Synopse zur ePrivacy-Verordnung. Zuletzt abgerufen von https://www.lda.bayern.de/media/eprivacy_synopse.pdf am 03.01.2019

Becher, M. (2009). *XML: DTD, XML-Schema, XPath, XQuery, XSLT, XSL-FO, SAX, DOM* (1. Auflage). Herdecke Dortmund: Springer Campus.

Bedner, M. & Ackermann, T. (2010). Schutzziele der IT-Sicherheit. In: *Datenschutz und Datensicherheit (DuD)*, *34*(5), S. 323–328.

Bell, D. E. & LaPadula, L. J. (1976). Secure computer system: Unified exposition and multics interpretation. Bedforde, United States.

Bergmann, H. (2009). Angeschnallt und los! Die Gurtdebatte der 1970er und 1980er Jahre in der BRD. In: *Technikgeschichte*, *76*(2), S. 105–130.

Bergt, M. (2015). Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag. In: *Zeitschrift für Datenschutz*, (8), S. 365–371.

Berkau, C. (1998). Instrumente der Datenverarbeitung für das effiziente Prozesscontrolling. In: *Kostenrechnungspraxis, Sonderheft 2*. S. 27–3.

Beutelspacher, A. (2008). Warum wendet man ausgerechnet Mathematik an? In: *„In Mathe war ich immer schlecht …“*. S. 166–177. Vieweg+Teubner.

Biba, K. J. (1977). Integrity considerations for secure computer systems. Bedforde, United States.

Biskup, J. (1993). Sicherheit von IT-Systemen als „sogar wenn – sonst nichts – Eigenschaft“. In: *Verläßliche Informationssysteme*. S. 239–254. Wiesbaden: Vieweg+Teubner.

Bizer, J. (2007). Modernisierung des Datenschutzes: Vier Säulen des Datenschutzes. In: *Datenschutz und Datensicherheit (DuD)*, *31*(4), S. 264–266.

Brinkkemper, S. (1996). Method engineering: engineering of information systems develop-ment methods and tools. In: *Information and Software Technology*, *38*(4), 275–280.

Broadnax, B., Mechler, J., Müller-Quade, J., Nagel, M. & Rill, J. (2017). Sicherheit relativ definieren. In: *Datenschutz und Datensicherheit (DuD)*, *41*(1), S. 24–28.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2018). *IT-Grundschutz-Kompendium* (1. Auflage). Köln: Bundesanzeiger Verlag.

Buchner, B. & Kühling, J. (2017). Die Einwilligung in der Datenschutzordnung 2018. In: *Datenschutz und Datensicherheit (DuD)*, *41*(9), S. 544–548.

Buchner, B. & Petri, T. (2018). DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung. In: J. Kühling & B. Buchner (Hrsg.), *Datenschutz-Grundverordnung / BDSG - Kommentar* (2. Auflage). München: C. H. Beck.

Bundesdruckerei, Kantar Emnid (2017). Digitialisierung und IT-Sicherheit in deutschen Unternehmen. Eine repräsentative Untersuchung. Zuletzt abgerufen von https://www.bundesdruckerei.de/system/files/ dokumente/pdf/Studie-Digitalisierung_und_IT-Sicherheit.pdf am 03.01.2019

BVerfG (Hrsg.) (1984). Urteil vom 15. Dezember 1983 aufgrund der mündlichen Verhandlungen vom 18. und 19. Oktober 1983 (1 BvR 209. 269, 362, 420, 440, 484/83). Volkszählungsgesetz 1983. In: *Entscheidungen des Bundesverfassungsgerichtes* (Band 65). S. 1–71. Tübingen: J.C.B. Mohr.

BVerfG (Hrsg.) (2008). Urteil vom 27. Februar 2008 (1 BvR 370). In: *Entscheidungen des Bundesverfassungsgerichtes* (Band 120). S. 274–350. Tübingen: Mohr Siebeck.

Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.). (2017). Kurzpapier Nr. 3: Verarbeitung personenbezogener Daten für Werbung. Zuletzt abgerufen von https://www.lda.bayern.de/media/dsk_kpnr_3_werbung.pdf am 03.01.2019

Decker, M. (2011). Modellierung ortsabhängiger Zugriffskontrolle für mobile Geschäftsprozesse. Karlsruhe: KIT Scientific Publishing.

Desel, J., Oberweis, A., Zimmer, T. & Zimmermann, G. (1997). Validation of information system models: Petri nets and test case generation. In: *Computational Cybernetics and Simulation 1997 IEEE International Conference on Systems, Man, and Cybernetics.* S. 3401–3406.

Dierstein, R. (2004). Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit. In: *Informatik Spektrum*, *27*(4), S. 343–353.

DoD, U.S. Department of Defence. (1985). *DoD 5200.28-STD Trusted Computer System Evaluation Criteria*. Zuletzt abgerufen von http://csrc.nist.gov/publications/history/dod85.pdf am 09.08.2018

Eckert, C. (2018). *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (10. Auflage). Berlin: De Gruyter.

Ernst, S. (2017). Die Einwilligung nach der Datenschutzgrundverordnung. In: *Zeitschrift für Datenschutz*, 7(3), S. 110–114.

Ernst, S. (2018). DS-GVO Art. 2 Sachlicher Anwendungsbereich. In: B. Paal & D. Pauly (Hrsg.), *Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (2. Auflage). München: C. H. Beck.

Eschholz, S. (2017). Big Data-Scoring unter dem Einfluss der Datenschutz-Grundverordnung. In: *Datenschutz und Datensicherheit (DuD)*, *41*(3), S. 180–185.

Europäische Kommission (2010). Gesamtkonzept für den Datenschutz in der Europäischen Union. Zuletzt abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52010DC0609 am 03.01.2019

Ferraiolo, David F. & Kuhn, D. R. (1992). Role-based access control. In: *Proceedings of the NIST-NSA National (USA) Computer Security Conference*. S. 554–563.

Fox, D. (2011). Betriebswirtschaftliche Bewertung von Security Investments in der Praxis. In: *Datenschutz und Datensicherheit (DuD)*, *35*(1), S. 50–55.

Freiling, F., Grimm, R., Großpietsch, K.-E., Keller, H. B., Mottok, J., Münch, I., Rannenberg, K. & Saglietti, F. (2014). Technische Sicherheit und Informationssicherheit. In: *Informatik Spektrum*, *37*(1), S. 14–24.

Frenzel, E. (2018). DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung. In: B. Paal & D. Pauly (Hrsg.), *Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (2. Auflage). München: C. H. Beck.

Gadatsch, A. (2015). Geschäftsprozesse analysieren und optimieren - Praxistools zur Analyse, Optimierung und Controlling von Arbeitsabläufen. Wiesbaden: Springer Vieweg.

Gola, P. (2018). Einführung. In: P. Gola (Hrsg.), *Datenschutz-Grundverordnung* (2. Auflage). München: C. H. Beck.

Gola, P., Jaspers, A., Müthlein, T. & Schwartmann, R. (2016). Datenschutz-Grundverordnung im Überblick: Informationen zur DS-GVO bei der Anwendung in der Privatwirtschaft Erläuterungen, Infografiken und Organisationshilfen. Frechen: DATAKONTEXT.

Grochla, E., Weber, H., Albers, F. & Werhahn, T. (1983). Ein betriebliches Informationsschutzsystem – Notwendigkeit und Ansatzpunkte für eine Neuorientierung. In: *Angewandte Informatik*, *25*(5), S. 187–194.

Gruhn, V. & Haack, B. (1995). Geschäftsprozeß-Management und Qualitätssicherung am Beispiel des WIS-Projekts. In: *Wirtschaftsinformatik '95*. S. 115–130. Physica, Heidelberg.

Hammer, V. (1999). Verletzlichkeitsreduzierende Technikgestaltung. In: *Verläßliche Informationssysteme*. S. 187–202. Vieweg+Teubner.

Hardin, R. (2002). *Trust and trustworthiness*. New York: Russell Sage Foundation Verlag.

Harms, J. M. (2011). Sicherheitsgewinn mit technologischen Innovationen (Schwerpunkt ITK). In: P. Zoche, S. Kaufmann & R. Haverkamp (Hrsg.), Z*ivile Sicherheit – Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. S. 29–33. Bielefeld: transcript Verlag.

Heberlein, H. (2017). EU-DSGVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten. In E. Ehmann & M. Selmayr (Hrsg.), *Datenschutz-Grundverordnung* (1. Auflage). München: C. H. Beck.

Hedtstück, U. (2013). *Simulation diskreter Prozesse*. Springer Vieweg, Berlin, Heidelberg.

Hemriti, H. (2011). Evaluierung eines Bestandsinformationssystems mit aktiven RFID-Transpondern in ‚Retailer Integrated E-commerce'-Lösungen (Diplomarbeit). KIT.

Herbst, T. (2018). DS-GVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten. In: J. Kühling & B. Buchner (Hrsg.), *Datenschutz-Grundverordnung / BDSG - Kommentar* (2. Auflage). München: C. H. Beck.

Hilbert, M. (2015). *Quantifying the Data Deluge and the Data Drought*. SSRN Scholarly Paper No. ID 2984851). Rochester, New York: Social Science Research Network.

Hoeren, T. (2018). Kirchlicher Datenschutz nach der Datenschutzgrundverordnung – Eine Vergleichsstudie zum Datenschutzrecht der evangelischen und katholischen Kirche. In: *Neue Zeitschrift für Verwaltungsrecht*, 37(6), S. 373–375.

Holten, R. (2000). Entwicklung einer Modellierungstechnik für Data-Warehouse-Fachkonzepte. In: *Modellierung betrieblicher Informationssysteme. Proceedings der MobIS-Fachtagung*, S. 3–21.

Hornung, G. & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. In: *Computer Law & Security Review*, *25*(1), S. 84–88.

Huch, S. (2016). Fallbeispiele innovativer Fintech-Unternehmen. In: *Wirtschaftsinformatik & Management*, *8*(3), S. 64–73.

International Organization for Standardization (2011). ISO/IEC 15909-2:2011: Systems and software engineering -- High-level Petri nets -- Part 2: Transfer format.

International Organization for Standardization (2014). ISO/IEC 27000:2014 (E) Information technology – Security techniques – Information security management systems – Overview and vocabulary.

Jandt, S. (2017). Datenschutz durch Technik in der DS-GVO. In: *Datenschutz und Datensicherheit (DuD)*, *41*(9), S. 562–566.

Jeanneret, C., Glinz, M. & Baar, T. (2012). Modeling the Purposes of Models. In: E. J. Sinz & A. Schürr (Hrsg.), *Modellierung 2012, 14.-16. März 2012, Bamberg, Deutschland*. S. 11–26.

Jensen, K. (1987). Coloured petri nets. In: W. Brauer, W. Reisig & G. Rozenberg (Hrsg.) Petri Nets: Central Models and Their Properties. Lecture Notes in Computer Science (Band 254). S. 248–249. Berlin, Heidelberg: Springer.

Jung, A. (2018). Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO. In: *Zeitschrift für Datenschutz*, 8(5), S. 208–213.

Karagiannis, D. & Kühn, H. (2002). Metamodelling platforms. In: *Proceedings oft he Third International Conference EC-Web* (LNCS Band 2455). S. 182–196.

Kaschek, R. (1999). Was sind eigentlich Modelle? In: *EMISA FORUM* (9), S. 31–35.

Kieck, A. & Pohl, D. (2017). Zum Anwendungsbereich des europäischen Datenschutzrechts. In: *Datenschutz und Datensicherheit (DuD)*, *41*(9), S. 567–571.

Klabunde, A. (2017). EU-DSGVO Art. 4 Begriffsbestimmungen. In: E. Ehmann & M. Selmayr (Hrsg.), *Datenschutz-Grundverordnung* (1. Auflage). München: C. H. Beck.

Klar, M. (2018). DS-GVO Art. 3 Räumlicher Anwendungsbereich. In: J. Kühling & B. Buchner (Hrsg.), *Datenschutz-Grundverordnung / BDSG - Kommentar* (2. Auflage). München: C. H. Beck.

Klein-Hennig, M. & Schmidt, F. (2017). Zurück auf Los – Die IT-Sicherheit zurück in der Steinzeit. In: *Datenschutz und Datensicherheit (DuD)*, *41*(10), S. 605–611.

Knorr, K. (2001). Multilevel security and information flow in Petri net workflows. In: *Proceedings of the 9th International Conference on Telecommunication Systems.* S. 613–615.

Körber, T. (2016). Ist Wissen Marktmacht? – Überlegungen zum Verhältnis von Datenschutz, „Datenmacht“ und Kartellrecht. In: T. Körber & U. Immenga (Hrsg.), *Daten und Wettbewerb in der digitalen Ökonomie*. S. 81–122. Baden-Baden: Nomos.

Körner, M. (2000). Informierte Einwilligung als Schutzkonzept. In: D. Simon & M. Weiss (Hrsg.), *Zur Autonomie des Individuums*. S. 131–150. Baden-Baden: Nomos.

Kübler, H.-D. (2018). Internet-Konzerne. In: R. Voigt (Hrsg.), *Handbuch Staat*. S. 1837–1847. Wiesbaden: Springer.

Kugelmann, D. (2018). Datenschutz im Mehrebenensystem. In: *Digitalisierung in Recht, Politik und Verwaltung*. S. 27–38. Baden-Baden: Nomos.

Kühling, J. & Raab, J. (2018). DS-GVO Art. 2 Sachlicher Anwendungsbereich. In: J. Kühling & B. Buchner (Hrsg.), *Datenschutz-Grundverordnung / BDSG - Kommentar* (2. Auflage). München: C. H. Beck.

Landwehr, C. E., Heitmeyer, C. L. & McLean, J. (1984). A security model for military message systems. *ACM Transactions on Computer Systems*, *2*(3), S. 198–222.

Leeb, C.-M. & Liebhaber, J. (2018). Grundlagen des Datenschutzrechts. In: *Juristische Schulung*, (6), 534–538.

Leimeister, J. M. (2015). *Einführung in die Wirtschaftsinformatik*. Berlin, Heidelberg: Springer Gabler.

Lenz, K. & Oberweis, A. (2003). Inter-organizational Business Process Management with XML Nets. In: H. Ehrig, W. Reisig, G. Rozenberg & H. Weber (Hrsg.), *Petri Net Technology for Communication-Based Systems*. S. 243–263. Berlin Heidelberg: Springer.

Leutheusser-Schnarrenberger, S. (2016). Die Bedeutung der Informationstechnologie für die Wirtschaft im Spannungsfeld mit den Rechten der Nutzer und Kunden. In: C. Bär, A- Fischer & D. Kempf (Hrsg.), *Informationstechnologien als Wegbereiter für den steuerberatenden Berufsstand.* S. 131–138. Berlin, Heidelberg: Springer.

Leutheusser-Schnarrenberger, S. (2017). Eine Digitalcharta für Europa. In: M. Schröder & A. Schwanebeck (Hrsg.), *Big Data - In den Fängen der Datenkraken*. S. 123–136. Baden-Baden: Nomos.

Leuze, R. (1980). Erster Tätigkeitsbericht der Landesbeauftragten für den Datenschutz. Landtag von Baden-Württemberg. Zuletzt abgerufen von https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/Taetigkeitsbericht/01.-Taetigkeitsbericht-1980.pdf am 03.01.2019

Lunt, C. (2017). Authorization and authentication based on an individual's social network US-Patent Nr. *US9798777B2*.

Martini, M. (2009). Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts. In: *Juristische Arbeitsblätter*, (12), S. 839–845.

Mauser, S. & Eggendorfer, T. (2017). Detecting Security Attacks by Process Mining. In: E. Kindler & R. Bergenthum (Hrsg.) *Algorithms and Tools for Petri Nets - Proceedings of the Workshop AWPN 2017.* S. 33–38.

McLean, J. (1985). A comment on the 'basic security theorem'of Bell and LaPadula. In: *Information Processing Letters*, *20*(2), S. 67–70.

Merschbacher, A. (2018). IT-Sicherheit. In: *Sicherheitsfibel*. S. 501–511. Springer Vieweg.

Morais, R. de, Kazan, S., Pádua, S. & Costa, A. (2014). An analysis of BPM lifecycles: from a literature review to a framework proposal. In: *Business Process Management Journal*, *20*(3), S. 412–432.

Müller, S. (2013). Der Schutz von Unternehmensgeheimnissen. In: J. Ensthaler & P. Wege (Hrsg.), *Management geistigen Eigentums: Die unternehmerische Gestaltung des Technologieverwertungsrechts.* S. 111–136. Berlin, Heidelberg: Springer.

Nef, W. (1977). *Lehrbuch der linearen Algebra (2. Auflage)*. Basel, Stuttgart, Birkhäuser.

Oberweis, A. (1990). *Zeitstrukturen für Informationssysteme*. Mannheim: Universität Mannheim.

Oberweis, A. (1996). Modellierung und Ausführung von Workflows mit Petri-Netzen. Stuttgart: Teubner.

Oberweis, A., Seib, J. & Lausen, G. (1991). PASIPP: Ein Hilfsmittel zur Analyse und Simulation von Prädikate/Transitionen-Netzen. *Wirtschaftsinformatik*, *33*(3), S. 219–230.

Pfleeger, C. P. & Pfleeger, S. L. (2003). *Security in Computing* (3. Auflage). Upper Saddle River, NJ, USA: Prentice Hall PTR.

Piltz, C. (2018). Verhandlungen zur ePrivacy-Verordnung - die wichtigsten Knackpunkte. In: *Der Betrieb,* 71(13). S. 749–752.

Pohl, H. (2004). Taxonomie und Modellbildung in der Informationssicherheit. In: *Datenschutz und Datensicherheit (DuD)*, *28*(11), S. 678–685.

Pohl, K. (2008). *Requirements Engineering: Grundlagen, Prinzipien, Techniken* (2. Auflage). Heidelberg: dpunkt.Verlag GmbH.

Pötters, S. (2018). DS-GVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten. In: P. Gola (Hrsg.), *Datenschutz-Grundverordnung* (2. Auflage). München: C. H. Beck.

Priese, L. & Wimmel, H. (2008). *Petri-Netze*. Berlin, Heidelberg: Springer.

Raabe, O. & Wagner, M. (2016). Verantwortlicher Einsatz von Big Data. In: *Datenschutz und Datensicherheit (DuD)*, *40*(7), S. 434–439.

Reimer, P. (2017). DSGVO Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten. In: G. Sydow (Hrsg.), *Europäische Datenschutzgrundverordnung* (1. Auflage). München: C. H. Beck.

Reisig, W. (1986). *Petrinetze*. Berlin, Heidelberg: Springer.

Reisig, W. (2010). Petrinetze: Modellierungstechnik, Analysemethoden, Fallstudien. Wiesbaden: Vieweg+Teubner.

Schaar, P. (2017a). Datenschutz-Empowerment. In: F. Abolhassan (Hrsg.), *Security Einfach Machen*. S. 23–30. Wiesbaden: Springer Gabler.

Schaar, P. (2017b). Wie die Digitalisierung unsere Gesellschaft verändert. In: M. Schröder & A. Schwanebeck (Hrsg.), *Big Data - In den Fängen der Datenkraken.* S. 105–122. Baden-Baden: Nomos.

Schalles, C., Rebstock, M. & Creagh, J. (2010). Ein generischer Ansatz zur Messung der Benutzerfreundlichkeit von Modellierungssprachen. In: G. Engels, D. Karagiannis & H. C. Mayr (Hrsg.), *Modellierung 2010*. S. 15–30. Klagenfurt: Lecture Notes in Informatics.

Schiefer, G. (2015). *Sicherer mobiler Zugriff auf Unternehmensdaten*. Norderstedt: Books on Demand.

Schild, H. (2018). DS-GVO Artikel 4 Begriffsbestimmungen. In: S. Brink & H. A. Wolff (Hrsg.), *BeckOK Datenschutzrecht* (24. Auflage).

Schleusener, M. (2017). Personalisierte Preise im Handel – Chancen und Herausforderungen. In: *Praxis der Personalisierung im Handel.* S. 71–89. Wiesbaden: Springer Gabler.

Scholz, B. J. (2017). SGB III § 394 Erhebung, Verarbeitung und Nutzung von Daten durch die Bundesagentur. In: B. Mutschler, R. Schmidt-De Caluwe & P. Coseriu (Hrsg.), *Sozialgesetzbuch III* (6. Aufl.). Baden-Baden: Nomos.

Schönthaler, F., Vossen, G., Oberweis, A. & Karle, T. (2011). *Geschäftsprozesse für Business Communities: Modellierungssprachen, Methoden, Werkzeuge*. München: Oldenbourg Wissenschaftsverlag.

Schönthaler, F., Vossen, G., Oberweis, A. & Karle, T. (2012). *Business Processes for Business Communities: Modeling Languages, Methods, Tools*. Heidelberg, Dordrecht, London, New York: Springer.

Schuhr, J. C. (2006). Rechtsdogmatik als Wissenschaft.: Rechtliche Theorien und Modelle. (1. Auflage). Berlin: Duncker & Humblot.

Schulz, S. (2018a). DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung. In: P. Gola (Hrsg.), *Datenschutz-Grundverordnung* (2. Auflage). München: C. H. Beck.

Schulz, S. (2018b). DS-GVO Art. 7 Bedingungen für die Einwilligung. In: P. Gola (Hrsg.), *Datenschutz-Grundverordnung* (2. Auflage). München: C. H. Beck.

Schulz, S. (2018c). DS-GVO Art. 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft. In: P. Gola (Hrsg.), *Datenschutz-Grundverordnung* (2. Auflage). München: C. H. Beck.

Schulz, S. (2018d). DS-GVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten. In: P. Gola (Hrsg.), *Datenschutz-Grundverordnung* (2. Auflage). München: C. H. Beck.

Schuster, T. (2012). Modellierung, Integration und Analyse von Ressourcen in Geschäftsprozessen. Karlsruhe: KIT Scientific Publishing.

Selmayr, M. & Ehmann, E. (2017). Einführung. In: E. Ehmann & M. Selmayr (Hrsg.), *Datenschutz-Grundverordnung* (1. Auflage). München: C. H. Beck.

Shannon, C. E. (1949). Communication theory of secrecy systems. In: *Bell system technical journal*, *28*(4), S. 656–715.

Simitis, S. (2014). Einleitung: Geschichte – Ziele – Prinzipien. In: S. Simitis (Hrsg.), *Bundesdatenschutzgesetz* (8. Auflage). Baden-Baden: Nomos.

Skusa, M. & Thalheim, B. (2015). Kohärente Multi-Modell-Entwicklung. In: B. Thalheim & I. Nissen (Hrsg.), *Wissenschaft und Kunst der Modellierung*. Berlin, Boston: De Gruyter.

Sowa, A. (2017). Management der Informationssicherheit. In Reihe: W. Hower (Hrsg.), Studienbücher Informatik (Band 7). Wiesbaden: Springer.

Stach, C., Alpers, S., Betz, S., Dürr, F., Fritsch, A., Mindermann, K., Palanisamy, S., Schiefer, G., Wagner, M., Mitschang, B., Oberweis, A. & Wagner, S. (2018). The AVARE PATRON - A Holistic Privacy Approach for the Internet of Things. In: P. Samarati und M. Obaidat (Hrsg.), *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) – Volume 1 SECRYPT.* Porto, Portugal. S. 372–379.

Stachowiak, H. (1973). *Allgemeine Modelltheorie*. Wien: Springer.

Stolz, F. (2018). Integration von Prolog-Modulen in eine Microservice-Architektur (Masterarbeit). KIT.

Ström, P. (2005). Die Überwachungsmafia: Das gute Geschäft mit unseren Daten. München: Hanser.

Thalheim, B. & Nissen, I. (2015). Ein neuer Modellbegriff. In: *Wissenschaft und Kunst der Modellierung Kieler Zugang zur Definition, Nutzung und Zukunft*. Berlin, Boston: De Gruyter.

Thomas, O. (2005). *Das Modellverständnis in der Wirtschaftsinformatik: Historie, Literaturanalyse und Begriffsexplikation*. In Reihe: A.-W. Scheer (Hrsg.), Veröffentlichungen des Instituts für Wirtschaftsinformatik (Band 184). Saarbrücken: Deutsches Forschungszentrum für Künstliche Intelligenz.

Tortorella, G., Miorando, R. & Marodin, G. (2017). Lean supply chain management: Empirical research on practices, contexts and performance. In: *International Journal of Production Economics, 193*, S. 98–112.

Valmari, A. (1998). The state explosion problem. In: *Lectures on Petri nets I: Basic models*, S. 429–528.

van der Aalst, W. M. (1998). The Application of Petri Nets to Workflow Management. In: *Journal of circuits, systems and computers*, *8*(1), S. 21–66.

van der Aalst, W. & Stahl, C. (2011). *Modeling business processes : a petri net-oriented approach*. Cambrige (Massachusetts), London: MIT Press.

van der Aalst, W. & van Hee, K. M. (2004). *Workflow management: models, methods, and systems*. Cambrige (Massachusetts), London: MIT press.

VanGundy, A. (1984). Brain writing for new product ideas: an alternative to brainstorming. In: *Journal of Consumer Marketing*, *1*(2), S. 67–74.

Veil, W. (2018). Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO? In: *Zeitschrift für Datenschutz*, 8(1), S. 9–16.

Verginadis, Y., Michalas, A., Gouvas, P., Schiefer, G., Hübsch, G. & Paraskakis, I. (2017). PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services. In: *Journal of Grid Computing*, *15*(2), S. 219–234.

Voßhoff, A. (2015). *Beibehaltung der 2-Säulen-Strategie als Garant für Vertrauen der Bürger, Kunden und Beschäftigte*. Vortrag, gehalten auf dem BvD-Symposium anlässlich des 20. Jahrestages der Richtlinie 95/46/EG, Nürnberg. Zuletzt abgerufen von https://www.bfdi.bund.de/SharedDocs/ Publikationen/Allgemein/VortragBvDSymposiumNuernberg.html am 03.01.2019.

Wagner, M. & Raabe, O. (2016). 7 Irrtümer zum Datenschutz im Kontext von Smart Data. In: *Datenbank-Spektrum*, *16*(2), S: 173–178.

Wendehorst, C. & Westphalen, F. (2016). Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht. In: *Neue Juristische Wochenschrift*, 69(52), S. 3745–3750.

Weppler, M. (2016). 100 Prozent Sicherheit – ein erstrebenswertes Ziel? In: F. Abolhassan (Hrsg.), *Was treibt die Digitalisierung?*, S. 141–147. Wiesbaden: Springer.

Wiese, L., Homann, D., Waage, T. & Brenner, M. (2018). Homomorphe Verschlüsselung für Cloud-Datenbanken: Übersicht und Anforderungsanalyse. In: H. Langweg, M. Meier, B. Witt & D. Reinhardt (Hrsg.), *Sicherheit 2018*. S, 221–234.

Winter, R. (2003). Modelle, Techniken und Werkzeuge im Business Engineering. In: H. Österle & R. Winter (Hrsg.), *Business Engineering*, S. 87–118. Berlin, Heidelberg: Springer.

Wolf, H. A. (2017). Die unterschiedlichen Kodifikationen des Datenschutzrechts. In: P. Schantz & H. A. Wolf (Hrsg.), *Das neue Datenschutzrecht - Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis* (1. Auflage). München: C. H. Beck.

Yaghmaei, E., van de Poel, I., Christen, M., Gordijn, B., Kleine, N., Loi, M., Morgan, G. & Weber, K. (2017). *Canvas White Paper 1 – Cybersecurity and Ethics* (SSRN Scholarly Paper No. ID 3091909). Rochester, NY: Social Science Research Network.

Zeuner, V. (2016). Ein Modell für Datenschutz durch Datensicherheit. In: *Datenschutz und Datensicherheit - DuD*, *40*(7), S. 452–457.

Zhu, H., Hall, P. A. V. & May, J. H. R. (1997). Software Unit Test Coverage and Adequacy. In: *ACM Computing Surveys*, *29*(4), S. 366–427.

Ziebarth, W. (2017). DSGVO Artikel 4 Begriffsbestimmungen. In: G. Sydow (Hrsg.), *Europäische Datenschutzgrundverordnung* (1. Auflage). München: C. H. Beck.

Zimmer, T. (2001). Petri-Netz-Konzepte für die Simulation verteilter betrieblicher Abläufe. Aachen: Shake

Es ist sinnvoll, **Datenschutz** und **Vertraulichkeit** nicht nur rein technisch zu betrachten, sondern diese Anforderungen in Organisationen bereits frühzeitig beim Entwurf von **Geschäftsprozessen** zu berücksichtigen. Um Prozessmodellierer und -verantwortliche dabei zu unterstützen, wurden als graphisches Darstellungsmittel **Informationsvertraulichkeits- und Datenschutz-Netze** entwickelt. Diese erweiterten **Petri-Netze** ermöglichen es, Vertraulichkeit und Aspekte des Datenschutzes innerhalb von Geschäftsprozessmodellen **systematisch** zu betrachten. Dazu wird die Geschäftsprozesssicht insbesondere mit der Organisationsstruktursicht und der Datenstruktursicht zu einer **integrierten Modellsicht** verknüpft. **Vertraulichkeit** wird im Zusammenhang mit den an der Geschäftsprozessausführung beteiligten Ressourcen (Organisationsstruktur) und den zur Ausführung benötigten Daten (Datenstruktur) in Informationsvertraulichkeits- und Datenschutz-Netzen entweder klassen- oder rollenbasiert betrachtet. Zweckbindung und Datenminimierung als spezielle Aspekte des **Datenschutzes** können mittels der Informationsvertraulichkeits- und Datenschutz-Netze ebenfalls beschrieben werden. Um die Anwendung zu unterstützen, wird die neue **PriCon4BPM-Methode** (Privacy & Confidentiality for Business Process Management) vorgeschlagen. Dabei werden die Schritte zur Erstellung der Informationsvertraulichkeits- und Datenschutz-Netze detailliert beschrieben. Zusätzlich wird eine durchgängige Vorgehensweise von der Modellierung bis zur Entscheidung (beispielsweise bezüglich Prozessalternativen) vorgestellt.

ISBN 978-3-7315-0933-2



Gedruckt auf FSC-zertifiziertem Papier